# Electronic Patient Record Security Policy in Saudi Arabia National Health Services

**Mouhamad Aldajani**

**This thesis is submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy**

**Software Technology Research Laboratory**

**(Faculty of Technology)**

**February 2012**

## ABSTRACT

Saudi Arabia is in the process of implementing Electronic Patient Records (EPR) throughout its National Health services. One of the key challenges during the adoption process is the security of EPR. This thesis investigates the current state of EPR security in Saudi Arabia's National Health Services (SA NHS) both from a policy perspective and with regard to its implementation in SA NHS's information systems.

To facilitate the analysis of EPR security, an EPR model has been developed that captures the information that is stored as part of the electronic record system in conjunction with stated security requirements. This model is used in the analysis of policy consistency and to validate operational reality against stated policies at various levels within the SA NHS. The model is based on a comprehensive literature survey and structured interviews which established the current state of practice with respect to EPRs in a representative Saudi Arabian hospital.

The key contribution of this research is the development and evaluation of a structured and model-based analysis approach to EPR security at the early adoption stage in SA, based on types of information present in EPRs and the needs of the users of EPRs. The key findings show that the SA EPR adoption process is currently proceeding without serious consideration for security policy to protect EPR and a lack of awareness amongst hospital staff.



**Key Words:** information security, Access control policy, EPR, Saudi Arabia.

## DECLARATION

I declare that the work described in my thesis is original work undertaken by me for the degree of Doctor of Philosophy, at the Software Technology Research Laboratory (STRL), De Montfort University, United Kingdom. No part of the material described in this thesis has been submitted for the award of any other degree or qualification.

## ACKNOWLEDGEMENT

In the name of God, the Most Merciful and the Most Gracious, I give praise and thanks to Him for supporting me with the strength to complete this research, and for providing me with knowledgeable and caring individuals during the study process. The researcher would like to express his deepest appreciation and gratitude to the research supervisor, Dr. Helge Janicke, for his dedicated help, time and valuable guidance through all the stages of this research project.

I would like to take this opportunity to thank Prof. Hussein Zedan, Prof. Bernd Stahl and Mark Shaw for their highly appreciated and valued help and support throughout my time at De Montfort University.

I owe special thanks to my family for their endless support, encouragement and prayers and, more importantly, their patience.

# TABLE OF CONTENTS

## **LIST OF** FIGURES

# LIST OF TABLES

# LIST OF ABBREVIATION

| | |
|---|---|
| **DCR** | Detailed Care Record |
| **EHR** | Electronic Health Record |
| **EPR** | Electronic Patient Record |
| **KFH** | King Faisal Hospital in Riyadh |
| **ICT** | Information and Communication Technology |
| **IS** | Information Security |
| **ISM** | Information System Management |
| **MIS** | Management Information System |
| **NHS** | National Health Services |
| **SA** | Saudi Arabia |
| **SA NHS** | Saudi Arabia National Health Services |
| **UN** | United Nation |
| **OECD** | Organisation of Economic Corporations and Development |
| **AHIMA** | American Health Information Management Association |
| **PHR** | Patient Health Record |

# CHAPTER ONE:

# INTRODUCTION

Objectives

- Justify and state the importance of the research.
- State the research aim and objectives.
- Highlight the original contribution and identify research aims and objectives.
- Outline the thesis organization.

# 1 CHAPTER ONE: INTRODUCTION

## 1.1 Introduction

Health services information has seen a shift in its recording, storing and transferring methods from a traditional, paper based approach to the use of electronic technology. Wider availability of information using electronic media in health services has led to concerns as to the security of health information and the possibility of security breaches. Health services information security has become critical for concerned stakeholders, including patients, clinical and non-clinical staff, suppliers and local communities, due to the need to comply with national and international regulations, and to the image of the health services.

There are several drivers for the need of national health services information security. These drivers include the improvement and promotion of quality of the health services (Marchibroda, 2007). The Security of Electronic Patient Record (EPR) helps to promote the quality of the services through safe handling of and access to patients' medical records. The second driver is the cost associated with the implementation of EPR information security in health services (Marchibroda, 2007; Protti et al, 2009). Use of Electronic Patient Record systems in health services requires purchasing hardware and software, as well as a change in the institutional infrastructure. These changes also require training programmes for the staff, which represent a cost to the health services. One of the other important costs that the SA NHS needs to consider is the cost of EPR security. The cost involves staff training in awareness, understanding and implementation of EPR security. The cost of development and implementation of appropriate security policy for EPR enforces security measures. Use of technology as a tool in securing EPR is another important source of cost.

This research focuses on the EPR system security in Saudi Arabia National Health Services, (SA NHS), and its policy to protect records. Information security policy in national health services should adequately protect any abuse of the system. (Straub and Nance, 1990) defined system abuse as the unauthorised, deliberate, and internally recognisable misuse of computers of any organisation's information system by individuals. It can be argued that the objective of information security is not only to

reduce personal abuse of the system as the security policy is more comprehensive in protecting data from internal, external and technology abuse.

Saudi Arabia Health Authority has implemented EPR systems in some of its hospitals and has a strategy to move towards implementing EPR systems throughout the national services. The purpose of this research is to explore and investigate EPR security in Saudi Health National Services and analyse the organisational information security policies while keeping the Saudi socio-political context in perspective. The proposed research will address both consistency of policies and conformance of organisational reality to these policies based on a formal modelling approach.

## 1.2 Research Aims and Objectives

This section presents the research main aim and objectives.

### 1.2.1 Research Aim

This research aims to explore, investigate and analyse the current state of electronic patient records security in Saudi Arabia National Health Services by addressing security at the policy level and developing information security framework to protect electronic patient record.

### 1.2.2 Research Objectives

The research aims can be achieved by carrying out the following objectives:

1. Investigation of the current situation of EPR in SA NHS.
2. Define main elements of EPR structure
3. Develop and design EPR security model.
4. Evaluate the developed EPR to ensure its usefulness, reliability and applicability to SA NHS
5. Analysis of EPR information security policy and to verify their consistency.
6. Exploring the main factors influencing adaptation EPR in SA NHS

## 1.3 Research Justifications

The use of EPR worldwide is increasing due to the development and availability of electronic technology and the awareness of its perceived importance and role in improving the quality of health services. One of the main challenges for implementing electronic information in a health services system is the security of the system. Within Saudi-Arabia, the Ministry of Health is making a gradual move from a paper-based record system to an electronic patient record system. Transition from a paper-based system to EPR is particularly challenging, due to the complex nature of the activities involved in maintaining health information and the large number of stakeholders involved.

This research aims to contribute to the understanding of electronic Information System Security in national health organisations. The outcomes of this research will particularly benefit the health services in Saudi-Arabia, as they are the key focus of the study.

## 1.4 Research Background

The E-health initiative in SA started in 2002 with the aim to improve its NHS and a meeting for this purpose was carried out to develop a national e-health plan for the Kingdom (Househ et al., 2010). It is well established that the SA government has a plan in implementing ICT in its institutions services such as the health services. The Ministry of Health envisaged savings of 10-15% of the public health budget by implementing an e-health strategy throughout the health services, and facilitating the progress of cooperative health insurance. The SA Ministry of Health invested 1.1 Billion USD in the implementation of e-health between 2008-2011 (SAHI, 2008). Among the main issues explored in literature conferences are information security, Kingdom e-health strategy, information policy and coordination among public health services organisations which are addressed in detail in Chapter 2.

Patient health providers are many and varied and due to lack of a unified system for patient medical records, this has meant that patient records are scattered among various health services providers (Altuwaijri, 2008). Altuwaijri went further by arguing the

lack of unified patients' medical records had led to waste of the health services' efforts and incurred financial consequences due to treating patients several times for the same health problems in several medical organisations (Altuwaijri, 2008).

There is a need to establish EPR security to protect the confidentiality, integrity, and availability of the EPR contents. The need has become more critical in SA due to the relatively recent awareness and education in SA towards their health services rights. The research is important to help the authority in developing and implementing EPR security policy.

SA NHS adopted a proprietary system to manage its health records in some of the hospitals. One of the main problems facing the SA NHS authorities is protecting the EPR. This is due to recent changes in understanding and awareness of patients' rights because of serious disputes between the SA NHS and insurance companies. The SA NHS has three ways of protecting EPR namely by law, by convention (policy) and by technology. The adaptation of the system in SA NHS is relatively new and the authority has failed to adopt strategies for protecting EPR. Currently there is a lack of national laws to protect EPR, which may be due to a lack of awareness and a lack of expertise to explore and establish such laws. The second problem is the absence of a clear policy to protect EPR. The currently adopted EPR policies appear to be generic, inconsistent and potentially insecure.

## 1.5 **Research Questions**

The outcomes of the research aim to provide answers and explanations to the research questions (Clough et al., 2007). The research formulated the following research questions:

Q1: What is the current situation of information systems security in SA NHS?

Q2: What are the main factors influencing Information Systems Security in SA NHS?

Q3: What is the structure of EPR and what information is contained within them?

Q4: What is the adopted security policy for protecting EPR?

Q5. Is the security policy translated into organisational reality?

## 1.6 Thesis Structure

The thesis is organised into the following chapters.

**Chapter 1: Introduction**

This chapter introduces the research aims and objectives, and provides justifications for the research. Moreover, it provides a brief introduction of the research context.

**Chapter 2: Literature Review**

The chapter establishes the research background. The chapter presents and critically reviews related research in the area of electronic patient records and the policies used to protect patient information.

**Chapter 3: Research Methodology**

This chapter presents the adopted research methods to answer the research questions. The data collection methods, sample selection, pilot study, and collected data methods are presented in the chapter.

**Chapter 4: Data Analysis: Interview Analysis**

The collected data is analysed and discussed in this chapter. The analysis is based on the issues explored and discussed in the oneto-one in-depth interviews carried out at SA NHS.

**Chapter 5: Modelling**

This chapter presents and discusses the developed EPR model and the information security model. The main purpose of the developed models is to be used in the analysis of access control to protect EPR information and EPR information security policies.

**Chapter 6: Evaluation access to EPR: Questionnaire analysis**

This chapter also presents a critical evaluation of the EPR model. The evaluation is based on the analysis of SA NHS responses to the developed model using a questionnaire to establish operational reality with respect to EPR security.

**Chapter 7: Discussions**

This chapter discusses the main outcomes of the research and critically evaluates the research results.

**Chapter 8: Conclusions**

This chapter summarises the research main contributions and recommendations to support on-going adaptation of EPR in SA NHS.

# CHAPTER TWO:

# LITERATURE REVIEW

Objectives

- Critically review and analyse the literature with respect to the research objectives.
- Review the definitions and terms used with respect to EPR and analyse the benefits and limitations of using EPR in health services.
- Review and analyse EPR structure, content and design and EPR information security policy.

# 2 CHAPTER TWO: LITERATURE REVIEW

This chapter discusses and analyses the literature related to security within the area of health information systems. The main purpose of this chapter is to understand the state of the art in health service security and to establish a research framework. The literature review will be linked to the outcomes of the data analysis in the discussion chapter.

"*Information and communication technologies have greatly affected the delivery of health care and lead to benefits in terms of quality and safety of patients*." (Steele, *2010)*

## 2.1 Introduction

The development in digital electronics in the last few decades has helped to develop hardware and software that can be used to improve health service organisations. Lucas (2008) argued that the development of the innovative regulatory mechanism is due to the development of ICT. The development of ICT has an impact on the health services knowledge management by providing technology that can be used as tool in knowledge management and information management systems.

The information systems in health services have attracted health services stakeholders to improve health services performances. One of the main challenges for the health information systems is security. The main driver for the challenge is the sensitivity and the importance of medical data and records. It is argued that the quality of healthcare data needs to address the security, privacy and confidentiality of the healthcare records due to two main concerns, namely transmission and access (Kahn and Sheshadri, 2008). However, Anderson et al., (2008) argued that privacy and confidentiality mean the same in medical usage.

The need for secure health information systems attracted academic and health services professionals to carry out research to establish the most appropriate approaches to promote the health information systems security; this is in order to help improve the health services.

Health services organisation policies and procedures in the health information systems security are important to ensure effectiveness of the security of the system. These policies and procedures require awareness, understanding and implementation to ensure effective secure operation of the systems.

The rapid expansion of electronic information services within the NHS (Kluge, 2007) and Saudi public health services has reinforced the need for effective security and confidentiality arrangements, to apply at multiple levels. The levels include management levels, clinical and non-clinical staff and the external stakeholders such as suppliers.

The chapter sections include electronic patient record definitions, electronic parent record benefits, limitations of EPR, EPR structure and contents, EPR information security, EPR information security policy, EPR ownership and EPR policy, national public health services in Saudi Arabia, and health information security in SA.

## 2.2 Electronic Patient Record (EPR) Definition

There are several terms used in the literature reflecting the use of electronic information in health services. One of the main challenges to the scholars in the health services is to accept and agree terms and definitions. There is no acceptance of the EPR definitions among universities in the USA (Hoffman, 2008; UK National Committee on vital Health and Statistics, 2006). This section briefly presents a definition of the electronic patient records and clarifies the term that will be adopted in this research.

### 2.2.1 Electronic Medical Record, EMR

Electronic medical record, EMR, has been used widely in the literature by scholars as well as in the health services organisations. The term defined EMR is defined as "*An electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorised clinicians and staff within one healthcare organisation*" (Wager et al., 2009).

### 2.2.2 Personal Health Care (PHS)

There are no major differences between the definition of EHR and the use of Personal Health Care in the literature. PH is defined as: "*An electronic record of health-related information on individual that conforms to nationally recognised interoperability*

*standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.*" (National Alliance for Health Information Technology, 2008). The definition again reflects individual information and data that can be used in health services processes and operations. The meaning of this definition does not differ from the EMR definition. This stresses the importance and the need for standardisation of terms and definitions of these terms.

### 2.2.3 Electronic Patient Record, EPR

Patient care is the centre of the health services activities. The services main aim is to meet patients' health care needs and satisfaction. Therefore, patient records are important records for the patient health care process and health services processes and information. Patient records are the core of the health services information management systems. Electronic Patient Record, EPR, is used in the literature without any agreement as to its specific definition.

The House of Commons Health Committee (2007) used the term and explored its main potential in health services. The committee stressed that PR has the potential to bring huge benefits to patients as well as to the health services organisations.

### 2.2.4 Electronic Health Record, EHR

Electronic Health Record, EHR, has been used widely in the literature. The main definition of this term is: "*EHR encompasses all health information in all media forms regarding an individual and is primary source for recording and documenting client health data*'' (Bickford and Hunter, 2006). Another definition of the term is provided by Wager et al (2009). They defined EHR as "*Electronic health record: an electronic record of health-related information on an individual that conforms its nationally recognised interoperability standards and that can be created, managed, and consulted by authorised clinicians and staff across more than one healthcare organisation*".

Again, the definitions of EHR reflect the individual information in various electronic formats. The definitions do not differ in principle from the EPR, MR and PHS. This stresses the importance and the need for standardisation in terms and definitions used in healthcare services and eliminates any interchange in using the terms as this leads to confusion in the use of the terms.

This research will use the term 'Electronic Patient Record' (EPR) throughout the research. The term reflects the electronic records of health-related information of patients in healthcare services. The records can be created and managed by the healthcare services and can be used by internal and external users.

## 2.3 Electronic Parent Record Benefits

The shift from traditional, paper based systems to electronic systems has its advantages and limitations based on the nature of the systems. It is important to analyse the advantages and limitations of adopting electronic patient records with regard to help making decisions and eliminate limitations wherever possible. This is important for countries such as Saudi Arabia which are in the process of adopting electronic patient records. The majority of the health services organisations in SA currently use the traditional recording process, paper based recording. John (2006) argued that using only a paper system in health services no longer makes sense due to the potential of the electronic patient record system and the limitations of the traditional recording system. The main limitations of the traditional patient record system include; patient data may not be recorded in a uniform fashion; paper may be lost or misplaced; difficulties may arise in sorting; and data cannot be accessed at different locations (Sridhar et al .,2009). These limitations with development in technology have encouraged healthcare service authorities worldwide, especially in developed countries, to implement an electronic patient record strategy in their healthcare services processes. Perera et al. (2011) provided evidence on the benefits and problems of electronic patient records. They argued that "it is essential that the risks of health information privacy loss be addressed minimised and monitored".

The following section explores the main advantages of EPR based on the main outcomes of the literature.

### 2.3.1 Benefits of EPR Implementations

There are several benefits of EPR implementation in healthcare services based on the potential and format of the EPR. The main identified benefits are based on the experience and outcomes of the literature survey. The following briefly presents the

main advantages of implementing EPR and the health services' needs to consider these advantages to help in decision making towards EPR strategy.

#### *2.3.1.1 Improve patient care, quality of healthcare*

The core of healthcare services is patient care and, therefore, the healthcare services processes and operations need to be focused to serve patient care. One of the main purposes of adopting electronic recording in health services processes is to improve the quality of patient healthcare (Wager et al. 2009; Sridhar et al., 2009; Lorenzi et al., 2009; Dekker wt al. 2007; Bakker, 2004). The record provides the basis of patient care process plan and treatment (Wager et al, 2009). Use of EPR in the patient healthcare process assists physicians and medical staff in the diagnosing and treatment of patients (House of Commons Health Committee, 2007). The committee also stated that electronic data has the potential to improve the quality of the healthcare audit and research of the health services.

#### *2.3.1.2 Reduce Errors*

One of the main challenges of health services is eliminating medical errors in the healthcare processes. Medical errors can lead to serious consequences to health organisations as many of the medical records can lead to patients' death. The number of deaths due to medical errors has been estimated to be as many as 98,000 deaths each year in the USA, at a cost of $29 billion (Hoffman et al., 2008).

Implementation of EPR helps in eliminating medical errors by providing all patients' medical information at any stage of the patient health care process (Sridhar et al., 2009; Jensen et al., 2006; John, 2007; House of Commons Health Committee, 2007).

#### *2.3.1.3 Universal Access to EPR*

One of the main limitations and disadvantages of using paper based recording is the difficulty in access patient records at various locations and at a convenient time. Use of EPR in health care helps to facilitate the access to EPR from several locations at convenient time and date of the patient and the medical staff (Sridhar et al., 2009).

The increased number of healthcare professionals involved in patient care also requires improvements in the cooperation and data exchange between them. An implementation

of EPR helps such cooperation (Haux , 2001; Meijden et al., 2000; Feldman et al., 2011)

#### *2.3.1.4 Administrative and Management Benefits*

The benefits of implementing EPR are not restricted to medical processes only but also extend to the healthcare services administrative and management processes. The administrative and management benefits include ease of scheduling and billing (Sridhar et al., 2009) improvements to the health services organisation's record management (Steele 2010) and improvements to organisational efficiency (Kannoju, et al., 2010; Lorenzi et al., 2009). Zhou et al., (2007) investigated the relationship between patient access to EPR with secure patient-physician messaging on primary care office visits. They found that the access decreased rates if primary care office visits and contacts,

#### *2.3.1.5 Efficiency and Integration of Medical Care Process*

One of the important elements of the patient care process is communication among patients' medical staff during the healthcare process. Huang et al., (2009) argued that patients' health records are distributed and located in different parts of the health care services organisation and clinics. They argued that one of the main problems is retrieving patients' information during patient visits to any department of the organisation. This is due to the difficulty of communication and accessing of patient records. The patient care process requires interaction by various medical professionals such as consultants, physicians and nurses. Patient records are a critical communication means for their communication about patients' medical care needs (Wager et al. 2009). Implementation of EPR can be shared by multiple providers of health services at different locations to improve the health quality of the patient care (Sridhar et al., 2009; Wainer, et al., 2008; Gordon et al., 2010).

#### *2.3.1.6 Research and quality management*

The nature and format of EPR help in medical and statistical research. EPR data and information can be used for research purposes and it can be used for monitoring the quality of care providers and sources of information and data for certain diseases (Wager et al., 2009; Abernethy et al., 2011). Hoffman et al. (2008) argued that EPR data and information promote medical research.

#### *2.3.1.7 Legal Advantages*

Patient records are needed in legal disputes and investigations. Patient records can provide evidence for legal support and argument. EPR can be considered as legal documents in cases of dispute and legal requirements (Sridhar et al., 2009). Therefore, it is important to stress the importance of EPR being electronically signed and identifiers being attached to any modifications to the records (Sridhar et al., 2009; Wainer, et al., 2008).

Patient records can become legal documents in the event of a lawsuit or other legal action involving a patient's records. Patient records can be used as primary evidence that a patient's medical history and treatment took place in the event of an accident (Wager et al. 2009).

#### *2.3.1.8 Patient Control*

The main purpose of the EPR is to serve the patient healthcare process. The EPR gives the patient control over his or her own healthcare process (House of Commons Health Committee, 2007).

## 2.4 Limitations of EPR

EPR implementation has several advantages and benefits to the health services, however, on the other hand there are several limitations of implementation of EPR in healthcare services. The following section presents the main limitations of EPR in healthcare services.

### 2.4.1 EPR does not Reflect Physicians Needs

Jensen et al. (2010) argued that one of the main limitations of implementing EPR in healthcare services is that EPR does not reflect the physicians needs. EPR provides little space for physicians to express their own ideas, opinions and the way they prefer to structure the patient's medical record. This may be due to lack of efficient and effective EPR design, from the point of view of structure, contents and design. This includes lack of grouping the patient's information based on the information sensitivity and importance in the patient's healthcare process.

### 2.4.2 Introducing EPR can be a Complex and Unpredictable Endeavour

One of the main reasons for EPR implementation failure is that, due to the complexity of the healthcare services, the personal health records of the individuals with health services become complex (Pagliari et al., 2007). Charles et al. (2010) explored the complexity of the healthcare services as a major challenge for adopting, modelling and security of EPR besides the sensitivity and diversity of the healthcare information.

Healthcare services consist of a large number of activities and processes. The processes are not simple and straightforward due to the nature of the activities and processes used. One of the main arguments for failing IS in health services is that the information systems underestimate the complexity of routine clinical and managerial processes.

Conflict between the high expectations of the systems commissioner, the system producer, and the health services users of the systems is also identified as one of the reasons for failure. Information systems implementation requires a long process in the health services sector. On the other hand, arguably, the managerial change and corporate memory is short (Littlejohns, 2003).

The shift from a traditional patent record system to an electronic patient record system can be a complex and unpredictable endeavour (Jensen et al., 2007). The transition period needs to be considered carefully due to the consequences of failure.

### 2.4.3 Patients' Access Rights

EPR will become more popular and patients will be more aware of its existence; this will increasingly make patients access their own EPR (Britto et al., 2009; Mandi et al., 2009). Perlin et al. (2004) argued that EPR can be a barrier to patients' right to access their own medical information records. They argued that patients' access to EPR is needed for patients' personal needs such as the patient's health planning and decision making. Ball et al. (2003) argued that the shift from the traditional, paper prescribing, practices to electronic recording could change who holds the main responsibility for protecting patients' privacy. They argued that the patient might no longer solely control the privacy of his or her data. On the other hand, Jian et al. (2011) went further by stating that the patient needs to carry his/her own records and by pointing out the needs of hospitals to provide information to the patient electronically.

### 2.4.4 Standardisation of EHR products and design

One of the main limitations of EPR implementation healthcare services is the lack of standardisation and design of EPR (Lorenzi et al., 2009; John, 2006). The literature indicates that there is no generic design, structure and contents for EPR that can be adopted by Saudi NHS services. It also indicates that there are several products developed by several companies for different health services organisations.

Charles et al. (2010) argued that the "*development in standardisation within e-healthcare, especially in the USA and Europe, have been motivated by patient-centred and managed care*".

Charles et al. (2010), argued that the standardisation of e-health main elements such as information, communication and security is an important determining factor for implementing e-health success. This is highly associated with the enactment and harmonisation of laws, policies and regulatory frameworks, (Charles et al., 2010).

### 2.4.5 Employees Resistance to change

The transition from traditional patient records to electronic patient records requires a change of employees' attitudes, awareness, behaviour, skills, knowledge and competence in order to cope with the shift from traditional to use of EPR. One of the limitations identified in the literature is the potential of employees' resistance to change (Lorenzi et al., 2009). Employees are not willing to learn new skills and competence that come with EPR implementations. The shift represents a change to their information seeking behaviour, recording process and the need to learn ICT skills. They are happy with what they are doing right now.

### 2.4.6 Organisation Culture

Littlejohns (2003) explained why computerised health information systems are prone to failure. He argued that one of the main drives for the failure is social and professional culture. Health services information systems failed to take into account social and professional cultures.

Charles et al. (2010) stressed people awareness as one of the important information security principles. "*Owners, providers and users of information systems should easily*

*be able to gain knowledge of and information about the existence and extent of security measures, practices and procedures*" (Charles et al., 2010).

The other principle stated is the ethics principle. They stated: "the security of information should be provided in such a way that respects the rights and legitimate interest of others" (Charles et al., 2010).

### 2.4.7 Information Security

One of the main limitations of EPR implementation is the patient's record information security. Rice (2008) argued that most of the e-healthcare information systems software is insecure. Jin et al. (2009) argued that EPR has significant patient sensitive information. Use of EPR allows accessibility to patient records at different locations and this increases the security of the information, possibly violating the patient's privacy and resulting in data theft. Alhaqbani et al. (2008) explore three main privacy issues due to the creation of EPR. These three main issues include patient desire not to grant access to certain information and data to a third party; the use of EPR may require the need to override privacy rule, especially in special circumstances; and "*the need to link only those records belonging to the same patient*". Dekker et al. (2007) argued that one of the main requirements EPR must fulfil is that of protecting patients' privacy and its contents must be kept confidential. On the other hand, Kahn et al. (2008) argued that the main constraint of EPR is in how to maintain data privacy and security.

Kahn et al. (2008) argued that the implementation of EHR systems in health services has two main security concerns. These concerns are transmission security and access security. The transmission security concern is based on ensuring the ability to transmit medical data and information safely and the security threat in the transmission process route. The access concern refers to the organisation's ability to ensure that the EPR records system is accessed only by those authorised to do so.

The other important point which needs to be stressed is the increase and growth of understanding and awareness of personal privacy and confidentiality of patients. Any breaches of privacy and confidentially poses major challenges to the health services (Charles et al., 2010). Charles et al. (2010) explored human factors as one of the security challenges facing healthcare services. Human factors include trust building,

patient consent, identify theft and Contain in confidentiality breaches. Geiger and Cranor (2006) "*raised the question of how much privacy protection we can realistically expect*''. However, increasing access to data through EPR systems also brings new risks to the privacy and security records (House of Commons Health Committee, 2007).

### 2.4.8 Cost and productivity

The initial office overhead cost is high due to the expensive hardware and software needed in the implementation of an EPR system (Kahn et al., 2008). The other cost explored in the literature is the physicians' productivity. Kahn, et al. (2008) argued that the physicians, at least initially, often become less productive when they implement an electronic record. Protection of privacy is generally recognised by:

- United Nations (UN)
- Organisation of Economic Co-operation and Development (OECD)
    - Guidelines governing the protection of privacy and trans-border flows of personal data (1980).
- Council of Europe and the European Community
    - Convention for the protection of individuals with regard to the automatic processing of personal data (1981).
- Irish Laws on protection of e-health information.
- The Data Protection Act (DPA) 1988 as amended by the 2003 Act. UK.
- The UK Data Protection Act (DPA), 1998. (Charles et al., 2010).

## 2.5 EPR Structure and Contents

Establishing right management systems in health services requires designing and structuring based on a right matrix. The matrix should be designed based on the healthcare services users, associated subjects, and main objects (data, functions, with appropriate access rights (Predeschly et al., 2008). The content and the design of an EPR system are not defined in a universal manner in the literature (Jensen et al., 2010). There is no agreement among scholars or healthcare services on the contents of EPR. This lack of agreement and design of EPR systems remains as one of the main challenges to the healthcare services. However, the American Health Information Management Association (AHIMA) proposed a list of the main contents of Patient

Health Record, (PHR). The association argued that the content components of EPR are common for most patients and they need to be included in the EPR design. These components include a patient's identification sheet, problem list, medication history and physical progress notes, consultations, physician's orders, imagine and X-ray reports, laboratory reports, patient's consent and authorisation, operative reports, pathology reports and discharge summary (Wager et al., 2009).

Although there is no agreement on a precise definition of EPR, there is an agreement on the main core elements of EHR functionalities. These include the following (Hoffman et al., 2008):

- Health information and data: display patients': lab test results, allergies, etc.
- Results management: provide patients': lab test results, allergies, etc.
- Order entry and management: Computerised \medication orders and other care instructions can reduce or eliminate lost orders.
- Decision support
- Electronic communication and connectivity: facilitate medical staff communication

## 2.6 EPR Information Security

Although security technology has advanced in recent times, the technology has fallen short of eliminating the challenge posed by the health services to secure e-health information (Charles et al., 2010). This stresses that the health services' main challenge remains developing and implementing an information security policy to ensure secure data and information within its internal and external activities. There are several drivers for establishing a national health service's information security policy. One of the most important drivers is to enhance and promote the quality of healthcare services, (Marchibroda, 2007) which is the core of the services aim. Security of health services records and data helps in the promotion of quality of the services through safe handling and accessing of medical records.

The other important challenge to health services is the inconsistencies and interoperability in the security systems used. This raises the difficulty and lack of consistence in establishing effective information security policy. Yu et al. (2007) raised

a challenge by stating "*Major deficiencies of EHR, management system used today are inconsistencies and interoperability in security system*" (Yu et al., 2007).

Huber (2008) explored several issues related to information security management systems (ISMS) that need to be considered and explored as part of the design and implementation process of EPR. These issues include technical issues. These issues are concerned with technology used that enables ICT applications and services, to accessing and using technology applications and services to serve the healthcare services operations and processes. It is also important to stress the short life cycle of the technology used in healthcare services and the need to update the systems in a relatively short time. The second issue is organisational issues. These issues are concerned with organisation handling of resources and management events, employees' issues and environmental issues (Saleh et al., 2007). These are internal issues within the organisation and the organisation needs to control such issues through effective use of policies and procedures in the issues explored.

Huber (2008) argued that an information security management system contains two levels. The first level is the system level and the second is the process level. The process level of the ISMS system has several sub-processes. These sub-processes include planning, development, implementation, evaluation and maintenance. The process level aims to provide the orchestration of the process-level's tasks (Huber et al., 2008). These processes and sub-processes need to be considered in EPR security implementation strategy.

From a human point of view, a challenge is the healthcare employee skills and competence in the e-health services environment. One of the tools to have an effective health services information systems security is by planning effective training for services employees at all levels of the services. Katsikas (2000) suggested three major categories for information systems security training, namely legal, regulatory, and ethical framework relevant to information systems security, information systems security policies, and information systems security controls.

### 2.6.1 Information Confidentiality, Integrity and Legal Value

The main focus of this study is on EPR information security. Information security definition is based on three main characteristics, confidentiality, integrity and availability of the information (Gollman, 1999; Harris, 2003; Ferreira et al., 2007). However others authors added other characteristics such as legal value (Wainer et al., 2008). This section reviews these characteristics to help gain an understanding of information security and to be used as basis in the study's arguments and discussions.

#### *2.6.1.1 Confidentiality of the Information*

It is important to distinguish between confidentiality and privacy as often they are used interchangeably but they do not have the same meaning and interpretation. Privacy can be defined as an individual's right to not have their private information exposed. On the other hand, confidentiality is defined as the "*prevention of unauthorised disclosure of the information limiting access to the information to authorised individual only*", (Ferreira, 2007). (Yu et al., 2007) argued that the confidentiality of the information "*is the single most important feature that is proved to be the most difficult on to implement with respect to existing practices and regulations for EHR protection*". They argued that one of the main reasons for the difficulty in implementing effective EPR in health services is due to two main constraints. The first constraint is an organisation constraint whereby the organisation has no capability to achieve the desirable level to secure EPR. The main consequence of such a constraint is the lack of trust on the IT infrastructure in sharing EPR. The second constraint is the need to include requirements of using appropriate and effective content encryption and secure key management solution. On the other hand, Wainer et al., (2008) stressed that patient records need to be considered as private and confidential records. They stressed that no unauthorised person should inspect the contents of the patient records.

Patients' and medical staff's personal records are private and confidential, (Wainer et al., 2008). Access to the patients and medical staff records must be accessed only by authorised staff. The security system requires confidentiality of the data and information exchanged between the electronic health records and the server in the health services activities. This may include encrypting the data and information (van der Linden, 2009: Gritzalis and Lambrinoudakis, 2004).

#### *2.6.1.2 Integrity of the Information*

Integrity of the information is one of the main characteristics of information security. Ferreira (2007) defined integrity of information as "*the prevention of unauthorised modification of the information*". Wainer et al. (2008) argued that the life of a patient may be dependent on the information and data in his/her record. This important role of the EPR raised the importance that only authorised people should have the right to access and change the information (Yu el., 2007; Wainer et al., 2008). This explores the severity and impact of EPR contains on the patient life, healthcare process, as well as morally. Unauthorised access to the EPR may have serious moral and ethical issues.

Patient records have integrity as they are critical for the patient. Therefore, only authorised people such as the GP has the right to access and edit the patient records. This content integrity of the record and its access should be controlled through a clear and effective policy. Integrity requirement is one of the key requirements of the information security requirement. This requirement stresses that a signature needs to be implemented for protecting information content integrity, availability

Availability of the information can be defined as the prevention of unauthorised withholding of the information (Wainer et al., 2008).

#### *2.6.1.3 Legal Value*

The patient record is data and information taken by the medical professional and therefore the data and information of the data has a value. Wainer et al. (2008) stated that "*the patient's records are the unadulterated, complete records of all actions taken by the health professionals on behalf of that patent and should be the definitive source of information about said action.*",

### 2.6.2 Factors Influencing Information Systems Security

There is a lack of empirical evidence about how human, organisational and technological factors impact information security management and little is known about the responsibilities and roles of security practitioners or the effectiveness of their tools and practices (Hawkey et al. 2008; Kotulic and Clark, 2004).

The factors influencing information systems security can be classified into three main factors. These factors are organisational, technological and cultural.

Knapp's et al. (2006) research is based on analysing responses of 220 certified information systems security professionals. Based on the outcomes of these responses they developed a survey instrument. The proposed model is based on using structural equation modelling (Knapp, et al., 2006). The developed model is based on three constructs, management support, security culture and policy enforcement. The organisation security culture is measured against the value employees place on the importance of security. It is also indicated that a culture that promotes good security practices is an important factor for having a secure information system. It is argued that good security behaviour of the organisation's employees should be part of an organisation's norm in doing their business. (Knapp, 2006) argued that any employees caught violating important security policies need to be appropriately corrected. This can be achieved by certain information security rules that can sanction the employees who break the rules. He also emphasised that employees who are repeat security offenders need to be disciplined, and termination is a consideration for employees who repeatedly break security rules.

Top management members within organisations are key decision makers and play a critical role in establishing the appropriate rules and building a security culture through establishing the right and appropriate processes and leading by example. In the process of establishing the policies and strategies, management needs to consider the national and international laws on privacy and the data protection act to ensure that they are not violating national laws and guidelines. Gerber et al. (2008) indicated the need to consider the individual privacy and data protection act in the national laws.

The duty of loyalty is evident in certain legal concepts, including: conflict of interest: individuals must divulge any interest in outside relationships that might conflict with the enterprise's interest. Duty of fairness when presented with a conflict of interest, the individual has an obligation to act in the best interest of all parties. Corporate opportunity when presented with inside information. Confidentiality: all matters involving the corporation should be kept in confidence until they are made public (Peltier, 2004)

## 2.7 EPR Information Security Policy

Information security policy has become an important element of organisation information security strategy. Peltier (2004) defined policy as "*high level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specific subject area*". The main objective of information security can be stated as "*to provide management direction and support for information security in agreement with business requirements and relevant laws and regulations*'' (ISO/IEC, 2005).

Information policy is focused on establishing the parameters of information access ensuring access to certain types of information (Jager, 2007). Organisation policy has become an essential part of organisation management strategy. Therefore, the term policy is commonly used and people are asked to implement the policy in the organisation. However, there is no generic definition for the term. Peltier (2004) argued that, by establishing appropriate policies, the organisation can take control of its destiny. Peltier (2004) defined policy as "*senior management's directives to create an information security program, establish its goals and measures, and largest and assign responsibilities*". The definition reflects the author's personal interest and background. Policy has its importance in health services due to the sensitivity of the data and information.

The goal of an information security policy is to maintain the integrity, confidentiality, and availability of information resources. Kahn (2008) argued that health service employees need to fully understand the health service security polices and understand their roles. Protti et al. (2008) explored the importance of the active role of physicians in clinical information systems. The security of the health services information system credibility depends on the information systems security policy (Kadam, 2007).

The information security policy is one of the most important documents in an organisation and must therefore be written with due care (Hone et al., 2002). Several focus policies that need to be established in health services are explored in the literature and need to be considered by health service organisations.

| | | |
|---|---|---|
| i. Broad Categories | ▪ Information security Governance | ▪ Organisation information security |
| ii. Policy management Phases | ▪ Risk assessment | ▪ Monitoring (Audits and automated tools) |
| | ▪ Policy development | ▪ Policy enforcement |
| | ▪ Policy approval | ▪ Policy review |
| | ▪ Policy awareness and training | ▪ Policy retirement |
| | ▪ Policy implementation | |
| iii. External influences | ▪ Economic sector | ▪ Legal and regulatory requirements |
| | ▪ Technology advances | ▪ External threats |
| | ▪ Industry standards | |
| iv. Internal influences | ▪ Senior management support | ▪ Technology architecture |
| | ▪ Business objectives | ▪ Internal threats |
| | ▪ Organisation culture | |

**Table 2-1 : Information security categories and classifications (Knapp et al. 2009)**

### 2.7.1 EPR Access Control

The first step in the health services in their EPR access control policy planning and implementation is identifying the main users of the EPR. Access should be based on the needs of the information in the patient's care process. There are large numbers of employees in health care services, especially in the centralised, public, NHS such as SA NHS and thus a need to establish EPR access based on their information needs. Lovis et al. (2007) identified EPR medical staff users based on their job role (Table 2.2).

| Medical staff EPR users |
|---|
| Head of service: Physician |
| Consultant - physician |
| Physician in charge of patient |
| Medical students |
| Physician -lab |
| Clinical research assistant |
| Medical Technician |
| Evaluator of medical direction |

**Table 2-2 : EPR medical staff users (Ref: Lovis et al., 2007)**

Beale et al. (2008) argued the need for establishing an access list as part of the information security. They argued that the access control must be relevant in terms of the EPR user's identity and time. The identity should be focused on who is delivering care in the patient care process and time represents the actual time during the patient care process.

The other important access control the health services needs to consider is the access control of access setting: data controller or a gate keeper. The gate keeper determines who has the right to make changes to the access control list, EPR users (Beale et al., 2008). Privacy levels with the EPR are critically important in access control policy. There is a need to classify the EPR contents based on its privacy. The other access control identified is usability control. The usability is defined as providing a default to the EPR users and exceptions to the default policy are then added (Beale et al., 2008)

The other important information security principles that health services need to consider include the following:

- Time-limitation of access: "*mechanism should be implemented that limit the time during which given health professionals can see the patient record*", (Beale et al., 2008)
- Record Merging: "*when more than one EHR is discovered for the same patient, and have to be merged into a single record, the access control list have to be re-evaluated and merged by the patient and potentially relevant carers*", (Beale et al., 2008)
- Non-repudiation: "*digital signing should be mandatory*" (Beale et al., 2008).
- Access logging: (Beale et al., 2008

In the access control list principles (Anderson, 1996) principle 1 stated: "*Each identifiable clinical record shall be marked with an access control list naming the people or groups of people who may read it and append data to it. The system shall prevent anyone not on the access control list from accessing the record in any way*".

Ferreira et al. (2007) believed that health care professionals, and patient support staff need to participate effectively in the development of access control policy. They argued

that participation can play a major role in eliminating a large proportion of access control. On the other hand, several studies indicated that physicians and patients express a desire to limit access to EPR among healthcare employees' in order to protect the privacy of the data (Adams, et al., 2004; Carman, et al., 1995).

#### *2.7.1.1 Single-sign on authentication services*

This requirement requires the EPR system user to present his/her credentials. This includes a user-id, password, digital certificates. The security system should discover and check the user identity the discovery and checking of a user identity (var der Linden , 2009: Gritzalis and Lambrinoudakis, 2004; Elemam eta al., 2011).

#### *2.7.1.2 Smart authorisation*

This is granting rights to the users. Local security agents, such as the police, are requested to decide whether to grant access to remote users on whom they have only limited information (var der Linden, 2009: Gritzalis and Lambrinoudakis, 2004). Acharya et al. (2010) stressed authentication as a "way to establish identity and trust among entities such as sender and receiver."

#### *2.7.1.3 Auditing*

Security agents, such as NHS inspectors, record and store in their logs all information necessary for system auditing (Gritzalis and Lambrinoudakis, 2004).

## 2.8 EPR Ownership and EPR Policy

One of the main arguments in electronic health information environment is the EPR ownership. This has legal implications and needs to be clarified and understood by all EPR stakeholders. Clarifying ownership helps in establishing and implementing information security, legal disputes, transmitting and accessing information security. The owner is defined as "*the creator of the information*" (van der Linden et al., 2009). Establishing the owner of information is important for the following reasons ( Haak et al., 2003)

- The owner is responsible for the availability of the information, (For the accuracy of the information)
- Protection against any unauthorised access to the information

- Held responsible in legal disputes.
- In case a patient decides to change GPs or hospitals.

| Owner | Definition |
|---|---|
| Source | Location where the data are stored |
| Origin | Location where the data are created |
| Manager | Person/entity responsible for the data (provide, protect) |
| Author | Person/entity responsible for the content of the information |
| Creator | Person generating the data and entering in the system. |

**Table 2-3 : Definition of EPR ownership (ref: van der Linden, 2009)**

Ross et al. (2003) stated that patients in health services are interested in accessing their medical record when they are offered the opportunity by the health services provider. However, they also stated rare patients are rare requested to read their medical record spontaneously

## 2.9 National Public Health Services in Saudi Arabia

A shift from traditional information recording processes such as using pen, paper, and human memory, to an electronic recording system requires a fundamental change in the way information is produced, accessed and shared (Househ et al., 2010). It has also been observed that Saudi patients' records are scattered in different forms at different care facilities (Househ et al., 2010). The author went further by stating the SA NHS lack proper health information applications.

The Saudi health service has seen significant progress and development in the last few decades. The main drivers for this significant improvement are due to the following main factors:

(i) Significant increase in oil production sale and revenue,
(ii) Awareness and ambitions of the authority to improve the Kingdom's health services,
(iii) Increase in number of Saudi competent, qualified and skilled manpower, in the health services profession, and
(iv) Increase in society awareness and health education.

The above drivers have helped to improve the health services significantly. The quality of the Saudi health services today has become well known and regarded as competent both in the region as well as worldwide. The Saudi health services adopt an e-health strategy to enhance the quality of the health care and contribute to reducing waiting times in the health services processes and reducing the cost of delivery. The Saudi health services have adopted information system to improve the quality of the service. (Abdul-gader, 1997) argued that economic, legal and cultural improvements have an effect on implementation of ISM in Arab Gulf countries such as Saudi Arabia. From the cultural point of view, the author argued that the consequences of the cultural issues include Islamic Sharia or teaching. In this variable, the author argued "*misconception about fate and free will: the future belongs to Allah (God) no man*". The second cultural issue is the Arabic language: technical capability in Arabic is not well developed. The leadership style is described as centralised and autocratic, with staff resistant to change and innovation and with favouritism and nepotism prevalent.

The Kingdom of Saudi Arabia introduced Electronic Medical Records as part of the health services management. The introduction of Electronic Medical Records helps to improve health services and is a catalyst and gold standard for developing health services (Chang et al., 2009; Williams and Boren, 2008; Porter et al., 2005). The improvement due to use of Electronic Medical Records helped to reduce patients' waiting, resulted in more effective use of hospital clinical and non-clinical staff time, and improved the flow of patient information in the patient care process in the hospital.

### 2.9.1 Health Information Security in SA

Abu Musa (2010) carried out a comprehensive information security analysis in a large number of organisations in SA including the health services. He found that information security is relatively new in SA. Most of the organisations in SA lack clear information security strategies or an information security policy in written format (Abu Musa, 2010). The author went further by stating "*alignment between Information security Governance and the organisation's overall business strategy is relatively poor and not adequately implemented.*" However, the author stressed that the majority of organisations recognise the role and importance of information security. Abu Musa's

research focused on generic information security for the traditional recording while the current research is focusing on EPR information security.

## 2.10 Summary

The national health services records and activities are large and complex due to an increase in living age, advance in health care processes and medications, and better health care services. These have led to an importance and need for an effective and efficient Health Information System to manage the services.

National health services need to benefit from the rapid development in digital electronics to improve their performance through implementation of electronic information systems in order to meet their patients' needs, satisfaction and in order to meet the expectations of the health authority by providing high quality services at an acceptable cost.

One of the main challenges and problems of adopting EPR in health services is protecting information, and many security issues are related to the use of EPR. The first step in protecting EPR and establishing an appropriate security policy is the need to agree on an appropriate definition of EPR. There are several terms and definitions used in the literature for EPR and there is no mutual agreement on the terms and definitions used in healthcare services information systems. The second problem identified in the literature is the EPR structure. There is a lack of generic EPR structure, content and design. This problem complicates the process for developing and establishing appropriate EPR information security policy. Information security policy needs to be consistent in itself and within the law. The literature also stressed the importance of enforcing EPR security policy.

Information security in SA NHS is relatively new and is progressing slowly. The SA NHS at organisation level and nationally lacks a clear information security policy for EPR or for traditional NHS records. There is also an increase in the Saudi public's awareness of their rights in health services and the importance of securing their personal records from any abuse or unauthorised access.

# CHAPTER THREE:

# RESEARCH METHODOLOGY

Objectives

- Justify and state the importance of the research.
- State the research aim and objectives.
- Highlight the original contribution.
- Identify appropriate data collection methods to achieve the research objectives and answer the research questions.
- Select the samples for the model's development and for the evaluation process.
- Design a pilot study to evaluate and assess the interviews and questionnaire design.
- Questionnaire to establish operational reality of EPR security.
- For comparison against policies.
- A qualitative measure of EPR security policy implementation.

# 3 CHAPTER THREE: RESEARCH METHODOLOGY

## 3.1 Introduction

This study adopts a formal approach in collecting and analysing policy in the national health services of Saudi Arabia. The case study collected data and information from the Saudi National Health Services to model Electronic Patient Record, EPR, and the information security and behaviour of staff and the organisation's information security policies. This research used in-depth interviews to collect data and information from key personnel within the Saudi NHS. The interviews aimed to identify and explore shortcomings in the electronic patient record design and its security policy in the Saudi NHS in order to take appropriate actions to bring about improvements needed to ensure compliance and consistency by all staff involved. A second survey of the Saudi NHS was also carried out. This used a questionnaire in order to evaluate models developed from the outcomes of the first survey of the research.

Figure 3.1 shows the flowchart of the research process. The research started by determining the initial research aims and objectives, providing a justification for the research and the main questions that the research would aim to answer. After determining the research aims and objectives, an extensive literature review was conducted with a focus on health services Information System Security, electronic patient records security and the main issues of current health services security. This helped to develop the research framework and to gain an understanding and awareness of current research in the area. This was followed by data collection from fieldwork. This concentrated on EPR structure, elements and design. Based on the outcomes of the collected data analysis, an EPR matrix was designed for further analysis. In order to evaluate the model, a second survey was carried out and data was collected. This was followed by discussing the study's main outcomes.

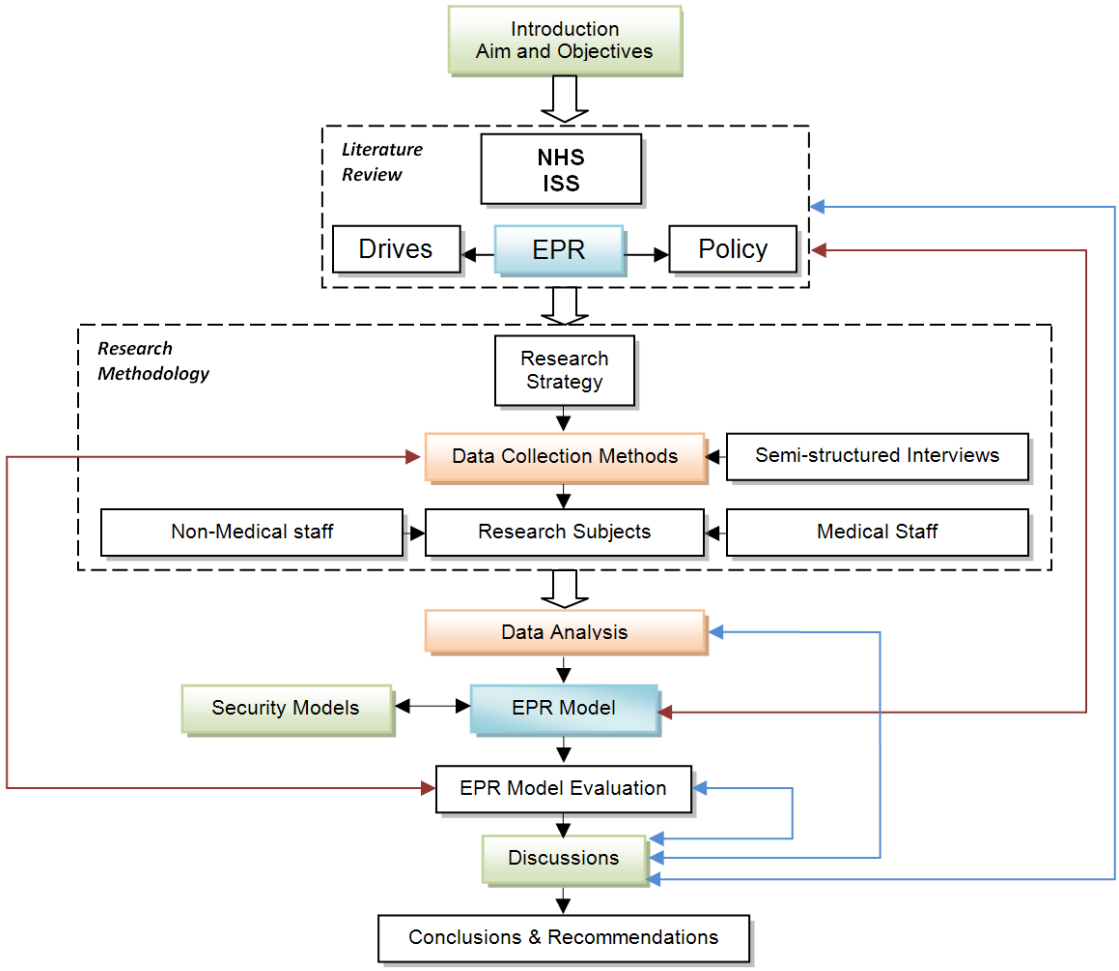



**Figure 3.1 : Research process flow chart**

## 3.2 Adopted Methods to Answer Research Questions

### 3.2.1 Review the Literature

The literature review developed the research framework and benefits from the previous research outcomes to serve the research objectives.

### 3.2.2 Data Collections

One of the tools used to achieve the research objectives and answer the research questions was collecting data from SA NHS. This is needed to provide raw data from the research fieldwork, hospital, to explore the current situation of EPR use and the policies used to protect the EPR contents. The data collection from the fieldwork was carried out in two stages. The first stage was collecting data and information that was

used in developing and designing the EPR record model and for the identification of existing policies. Semi-structured interviews were used to survey EPR users. The interviews aimed to explore hospital staff's opinions and attitudes towards the current use of EPR, EPR structure and the policies adopted to protect EPR. This stage helped in the process of developing EPR and identifying EPR structure to answer Research Question 3, "What is the structure of EPR?"

The second stage of data collection aimed to evaluate the developed EPR model. The data collection of this stage involved distributing a questionnaire to the EPR users to identify and explore their attitudes and behaviour towards EPR security. The evaluation process at this stage of the research was needed to check the practically, reliability and use of the developed EPR to SA NHS. Most importantly, the developed model can be used in analysing and developing information security to protect EPR.

### 3.2.3 Document Analysis

The SA NHS is one of the largest public services in SA. It has a large number of documents related to patient records. The main aim of the document analysis is to identify the information security policy with a special focus on EPR security. The SA NHS documents analysis was carried out at two levels. The first is the national level. This is needed due to the fact that SA NHS is a public sector organisation, managed, controlled and sponsored by the central government. This includes analysing the national policy with respect to health services information record security. The main aims at this level are analysing the Ministry of Health Services information security with a special focus on the EPR security policy. The second level is the health services organisations, hospitals, level. The aim is to analyse and identify statements with respect to hospital information security with a special focus on policies protecting EPR. This includes analysing hospital access control policy for accessing EPR and the consequences of any misuse and abuse to the integrity of the EPR contents.

SA NHS documents related to EPR security policy were analysed to identify its effectiveness and consistency. One of the main aims of selecting document analysis was in order to identify the current information security policy statements to protect the value and integrity of patients' records. This includes identifying the current access

control policy used at the health services organisations, hospitals, level. Document analysis is also needed to verify EPR security policy effectiveness and consistency.

The document analysis establishes the current situation of health services information security policy in SA NHS. The hospital EPR security policy document analysis helps in establishing whether the policy set by the organisation is translated into organisational practices and this helps to answer Research Question 5.

### 3.2.4 Modelling

One of the main objectives of this research is to develop models for EPR information security. A modelling approach was used to model EPR and EPR security policy and these models are presented in Chapter Five. These models were developed based on the main outcomes of the literature survey and analysis of data collected from the SA NHS. The collected data is mainly qualitative data, collected through structured interviews (see Chapter Four). This approach explored the SA NHS staff information needs and access to the EPR.

The EPR model was designed based on two considerations. The first was the type of patient information. The EPR information was divided by its nature and sensitivity. This was needed in analysing and developing EPR security policy by allowing the user to access the type of information they need based on the information security policy set by the hospital. This can be achieved by setting access control policy for each information type. The second consideration was users' profession. The users were divided by their profession and role in the patient care process at the hospital. Each profession needs certain data and information from the EPR based on their job roles and responsibilities in the patient's care process. This classification divides the users based on their profession and role on the patient's care process, used to design the structure of the EPR and most importantly in analysing and developing EPR security policy. The two developed models are presented in Chapter 5.

## 3.3 Work Packages

The research is carried out in five work packages. The packages are based on the research aim and objectives to facilitate the process of achieving the research objectives.

### 3.3.1 Work Package 1: Literature Review

This package focused on a critical review of the related literature to help in establishing the research framework. This is presented in Chapter 2. The literature review helps in developing the research framework, based on developing initial models for the health information security and a matrix for electronic patient records.

### 3.3.2 Work Package 2: Data Collection

This work package presents the data collection method that is adopted in this study to achieve the research aims and objectives. The data collection focused on two main tasks. The first task was collecting data and information regarding EPR and current information security policies. The method includes designing and carrying out one-to-one in-depth semi-structured interviews and document analysis. The research also collected data and information to evaluate the outcomes of the first survey. The second survey is based on designing a semi-structured questionnaire to collect data from SA NHS. The collected data was analysed using SPSS to evaluate the EPR content information needed by the SA NHS staff as well as the organisational reality with respect to EPR security.

### 3.3.3 Work Package 3: Data Analysis

The research was carried out in a fieldwork survey at a national health services organisation in Saudi Arabia. The survey collected qualitative and quantitative data. This package presents the critical analysis of the data to serve in developing and evaluating the research model. This includes a critical analysis of the one-to-one interviews and health services document analysis.

### 3.3.4 Work Package 4: Modelling

This work package presents the developed models. The first model developed is the Electronic Patient Record, EPR matrix. The model is based initially on the outcomes of the literature review and the field work data analysis. The model is needed to identify the information needed to be included in the EPR based on the SA NHS job role and to

group the information based on its sensitivity. The model is designed to reflect the real world of the SA NHS by involving the services in the design and evaluation processes.

## 3.4 Data Collection

This section presents and discusses the data collection methods used in this research, research samples, interviews for EPR design and content, questionnaire designs and process for evaluating the EPR design, and pilot study to check and test the interview and questionnaire designs.

This research adopts a formal approach in collecting and analysing EPR information security policy in the SA NHS. The study collected data from selected health services organisations to model electronic patient records and establish the behaviour of staff EPR access and the organisation's information security policies. Using the EPR (Chapter 6) model, the staff access behaviour (needs), and consistency with these policies in the SA National health services are analysed. This research used in-depth interviews to collect data and information from key personnel within SA NHS. This was mainly in order to achieve the development of a model for EPR security model that can be used to answer the research question, "What is the adopted security policy for protecting EPR?" The approach identifies and explores shortcomings in the information security system and its policy in the organisation in order to take appropriate actions to bring about improvements needed to ensure consistency by all staff involved.

### 3.4.1 Data Collection Methods

This section presents the data collection methods that were adopted in this research in order to achieve the research aims and objectives. The data collection focused on two main tasks. The first task was collecting data and information regarding EPR and the current information security policies used in SA NHS. The method includes designing and carrying out one-to-one in-depth semi-structured interviews and document analysis. The research also carried out a second survey, collecting data and information to evaluate the developed EPR security model. The survey identified the EPR user's access need to help develop EPR access control policy using a questionnaire to evaluate

the operational reality of EPR security against the policies and guidelines obtained from document analysis.

### 3.4.2 In-depth Semi-structured Interviews

This research requires collecting in-depth data and information to help in understanding EPR policies used in SA NHS. Qualitative methods are an appropriate approach for collecting in-depth data and information from King Faisal Hospital, KFH. KFH is one of the largest SA NHS hospitals and one of the few hospitals that have adopted EPR. This reflects a real-world scenario, in which data and information are based on the experience, knowledge, background and history of key personnel in the national health services.

### 3.4.3 Research Methods

Face-to-face in-depth interviews with key personnel in health services was carried out. In-depth face-to-face interviews help the researcher to explore, understand and discuss information systems security cultural issues (Sekaran, 1992). Face-to-face interviews also provide quotations and statements, from the interviewees based on their personal experience, opinions and knowledge (Patton, 2002). The main disadvantage of face-to-face interviews is subjectivity. Such interviews represent the interviewee's opinion and perception and possibly interview bias interferes with his/her own opinion and organisation (Sekaran, 1992; Drever, 2003). Face-to-face interviews can be designed as structured, unstructured or semi-structured interviews. Designing a structured interview is an appropriate data collection approach when the interviewer knows exactly what data and information he/she needs (Sekaran, 1992) and this is not the case in this research. On the other hand, the unstructured face-to-face interview has no control in the plan and process of the interviews (Sekaran, 1992). This is not appropriate to be adopted in this research due to the need to focus on the main research issues in order to to help to answer the research questions. Therefore, a mix of both in the form of semi-structured interviews will be adopted. The main reasons for adopting semi-structured interviews are due to their advantages in gathering factual information, collecting statements regarding individuals' opinions and exploring in depth interviewees' experience, reasoning, and motivation (Drever, 2003).

The interviews were designed to reflect the main research aims and objectives and focused on the following main issues:

- **Issue 1:** Current EPR information systems security policies in SA NHS.
- **Issue 2:** EPR Information system security access control
- **Issue 3:** Problems and obstacles in developing and implementing EPR information security.

### 3.4.4 Documentation Data Analysis

One of the methods used in collecting qualitative data is document analysis. Documentation represents an important source of data and information. (Creswell, 2003) stated several advantages of document analysis which can benefit this study. The advantages include: enabling the researcher to get information based on the participants' and organisation's language and the words they used in the security policy documents; the second advantage is that document analysis can be accessed and research carried out at their own convenient date and time. Document analysis saves the researcher effort, expenses and time compared with other methods of qualitative data collection methods.

The information system security policy documentations were investigated and analysed to identify any gap in the policies and to help in investigating the extent of its implication and compliance within the organizations. The documents analysed include:

- **EPR Information Security Policy:** The main documentation targeted is the hospital EPR information security policy (KFH Information Security, 2010). This is needed to identify consistency and compliance of the adopted policy. The research also analysed the SA Ministry of Health EPR information security policy and the process used in the establishment and adoption of such policies in SA NHS hospitals.
- **National and International IS policies:** The Ministry of Health is responsible for the Saudi NHS' activities, policies and activities (SA Ministry of Health, 2010). The Ministry IS policy will be analysed to assess its consistency and compliance in meeting national and international regulations and the NHS hospitals' needs and satisfactions.

## 3.5 Research Sample

Selecting a research sample is critical for the research outcomes, reliability of the collected data. Fink (2003) defined a research sample as:

"*a portion or subset of a larger group called a population*." (Fink, 2003)

The research focused on National Health Services in Saudi Arabia (see Figure 4.1). The figure shows the SA NHS with the main targeted groups and organisation. The sample is based on selecting one of the largest and one of the main hospitals that has adopted EPR into its operations, namely KFH. The selected sample is to serve the use of interviews, and questionnaire. The main subjects of the research are the KFH users of EPR. They can be classified as medical staff, non-medical staff and hospital management subjects.

### 3.5.1 The King Faisal Specialist Hospital and Research Centre (KFH)

KFH was selected in this study for the following reasons:

i. KFH is one of the first hospitals to introduce and implement EPR into its healthcare operations. This is one of the main reasons for selecting the hospital in this research as the vast majority of SA NHS still use a traditional, paper-based, recording system (KFH, 2010).

ii. There is not any research or studies in the hospital following the introduction and implementation of EPR to the hospital operations. The selection of the hospital provides the hospital authority with data and information that can be used on the EPR policy (KFH, 2010).

iii. KFSHRC is one of the largest specialised hospitals in SA NHS and has a 663-bed tertiary care facility. The hospital has 18 different medical departments providing medical health care services to the public with 6,946 staff from various cultural backgrounds (46% of whom are expatriates), with 63 different nationalities (KFH, 2010).

iv. The hospital introduced the Integrated Clinical Information System (ICIS) to improve the quality of the health care, reduce operational costs and increase utilisation of the hospital resources by making data available for research and analysis and improve communication process and information sharing

among hospital employees. The system also aims to improve the hospital operational efficiencies and improve patient safety. The introduced system also has a Computer-based Patient Record (CPR) aiming to eliminate use of the traditional, paper based record, unified patient record, ease accessibility to the information (KFH, 2010).

| | |
|---|---|
| Total number of patients admitted per year | 21,123 |
| Average daily inpatient census | 552 |
| Average bed occupancy rate | 88% |
| Average length of bed stay | 9.0 days |
| Average Outpatient encounters per year (excluding Emergency Room visits) | 516,875 |
| Average Emergency Room encounters per calendar day | 124 |

**Table 3-1 : Hospital initial data, (KFH, 2010).**

This research can argue that KFH is representative of other hospitals in SA NHS. This argument is based on the fact that KFH is one of the hospitals implementing EPR to its activities. It is also a fact that the SA NHS hospitals are public hospitals and have similarities in management and processes. EPR security is a common problem in SA NHS hospitals.

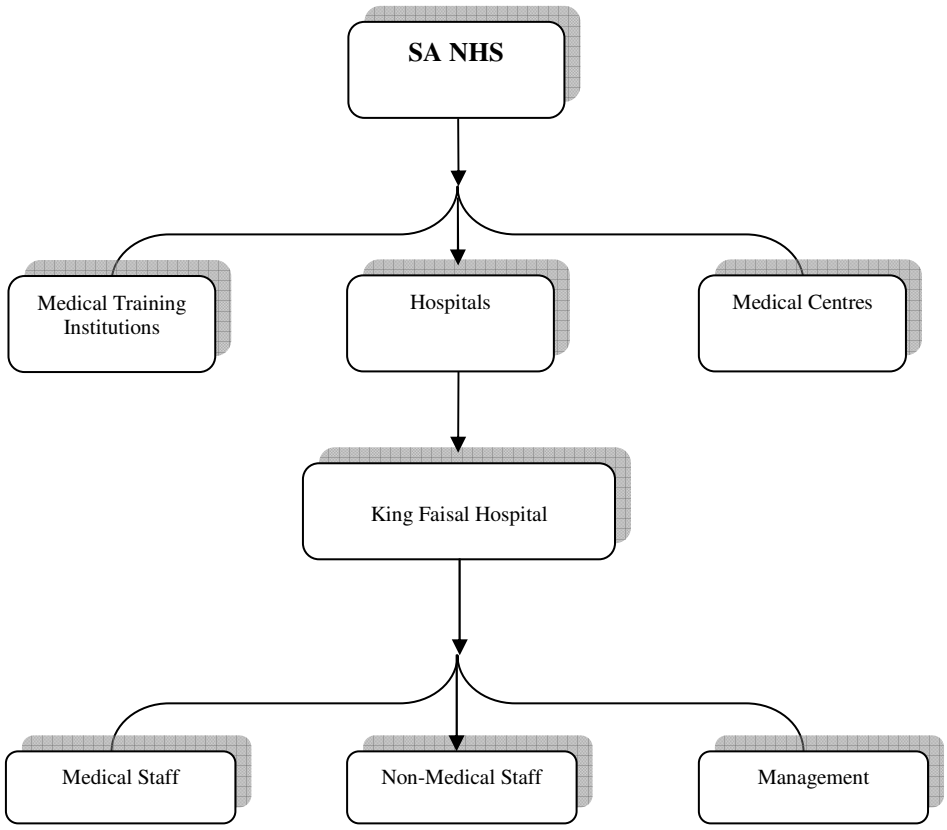



**Figure 3.2 : Research sample**

### 3.5.2 Research Subjects Sample

There are several staff members in the health services needing to access electronic patient records based on their role and responsibilities in the patient health care process. It is important to identify and explore the current main users of electronic patient record towards the current structure of EPR, access to EPR, security of EPR and their information needs. The outcomes of the survey were used in developing a model for EPR security which can be used for quantitative analysis.

McBurney et al. (2004) identified several types of samples that researchers need to consider during the sampling process. These samples include simple random samples, systematic samples, probability samples, convenience samples, haphazard samples, cluster samples and stratified samples. The most appropriate sample for this research is the stratified sample. A stratified sample is "a random sample in which two or more subsamples are presented according to some predetermined proportion, generally in the same proportion as they exist in the population" ( McBurney et al., 2004). In this research, the sample represents all the subgroups within the hospital such as there is a need to represent the medical doctors, nurse, and administrator and so on in the survey. This is due to the groups' role and responsibility in health care and their need to access electronic patient records. Once the research subjects are divided into groups based on their job activities, the subjects are selected randomly.

Table 3.2 shows the sample of subjects selected for interview and justifications for the selection. The total number of the sample was 15 subjects from various professions within the SA NHS.

| | Interviewed Subject | Main Justifications | No. |
|---|---|---|---|
| **1** | Managers | Decision Makers in Policy and regulations<br>Involved in ISM implementation and strategy.<br>Involved in any breach ISM security<br>Managing clinical and non-clinical staff | 1 |
| **2** | Medical Doctors-Physicians | Direct involvement in patient medical care<br>Needs to access EPR based on their jobs role and responsibilities | 2 |
| **3** | Medical Consultants | Main Decision maker in the patients' medical case.<br>Needs to access EPR based on their jobs role and responsibilities.<br>Needs to report to others EPR stakeholder if needed such as the patients employer | 2 |
| **4** | Nurse | Direct involvement in patient medical care<br>Needs to access EPR based on their jobs role and responsibilities. | 2 |
| **5** | Administrator/ Receptionists | First contact with patient-appointment<br>Involved in patient care management<br>Contact with patients' stakeholders such as their families | 2 |
| **6** | MIS Members (ICT Admin) | Implementing and maintaining EPR<br>Involved in staff training | 2 |
| **7** | Pharmacists | Part of the patient medical process.<br>Link between patients and physicians<br>Needs certain information to check and release patient medication | 2 |
| | | **Total** | 13 |

**Table** 3-2 **: Selected subjects sample**

The following section presents the main subjects and groups selected to participate in the survey and provides justification for the selection.

### 3.5.3 Hospital Senior Managers

The NHS is funded by the Saudi government and managed centrally by hospital managers and hospital senior managers who are appointed by the SA NHS. Therefore, it is critical to identify and explore hospital senior managers' opinions and attitudes towards EPR and its security. One hospital senior manager was selected.

#### *3.5.3.1 Director/Deputy of the Organisation*

They are selected to participate in the survey because they are decision makers, involved in the long- and short-term SA-NHS strategy. They were selected in order to understand their opinions and perception regarding EPR and information security issues.

#### *3.5.3.2 Senior Hospital Manager*

A senior hospital manager has been selected because the manager is involved in the decision making process and strategies. He is also responsible for the implementation of EPR, information security policy and regulation. The hospital manager is the line manager of the main users of EPR and is involved in analysing and resolving any information security issues within the hospital.

### 3.5.4 Medical Doctors (Physicians)

Medical doctors have an important role in the patient medical care process due to their job role and responsibilities. They need to access and update the EPR in the patient medical care process. Therefore, there is a need to examine and assess their opinions and perceptions towards EPR contents (information elements), access control, information types needed, information security and protection of the EPR record.

### 3.5.5 Medical Consultants

Consultants are the main users of the EPR due to their role and responsibility in making medical decisions on patients' medical cases. Medical consultants in the hospital lead a group of physicians in their medical specialisation. They need to access EPR in medical decision processes. Therefore, it is important to examine and assess their opinions and perceptions towards EPR information contents, EPR security, access control, and their information needs.

### 3.5.6 MIS Members

The Management Information System, (MIS) in the hospital is managed and maintained by a specialized team. They are trained in medical information system and ICT to provide support to the hospital medical and non-medical staff. The team is responsible for installing, updating, repairing and providing technical training and technical support for the hospital staff. Two MIS members have been selected to participate in the in-

depth interviews. One is an MIS professional and the second is a member of the MIS development team.

#### *3.5.6.1 ISM Professional*

An ISM professional has been selected to explore the technical aspects of EPR protection and their experience with the EPR users from the system security point of view. The interview was also an opportunity to explore the ISM professional's opinion and views on users' skills and competence in using the system and their awareness of the security and protection of the EPR system used in the hospital. The interview also served to explore their needs to access EPR.

#### *3.5.6.2 ISM Development Team (System Analyst Staff)*

A development team member provides data and information regarding the process and procedures used to ensure the EPR system security as well as technical information regarding security problems created by misuse of staff or any external internal intruder.

### 3.5.7 Administrators (Non-clinical staff)

There are several non-clinical staff who need to interact with patients during the patient medical care process in the hospital. Non-clinical staff include hospital administrators such as the main hospitals' and departments' receptionists. Non-clinical staff need to access and edit certain EPR information as part of their support process to the clinical staff. Therefore, there is a need to explore the non-clinical needs for accessing electronic patient records. Two hospital administrators have been selected to explore their opinions and views regarding EPR contents, access control and protection.

### 3.5.8 Pharmacists

Pharmacists are professionals who need to check a patient's identity and medications before advising the patient on medication taken and passing the medication to the right patients. A pharmacist may also need to contact the medical consultants and physicians in case of uncertainty in the medication or information provided in the subscription. Two pharmacists have been selected to explore and identify their opinion and views towards the EPR contents, access and EPR security.

## 3.6 Pilot Study

The designed semi-structured interviews need to be piloted and checke, before the actual interviews. McBurney et al. (2004) defined a pilot study as a "tentative, small-scale study done by pre-test and modify study design and procedures". This is needed to check accuracy and validity before the actual interviews occur. One of the main purposes of the pilot study is to check the accuracy of the interview question wordings. The pilot study works as a check for any fatal ambiguities and helps in devising the actual wording of the interview (Oppenheim, 1968). A pilot study was used in this research to help ensure appropriate wording of the interview questions used and to avoid any serious ambiguities. The pilot study also checked whether the interviewees' responses met the purpose of the questions. This gives an indication as to whether the questions' answers met the purpose of the questions. Finally, the pilot study helped to identify the most appropriate models and tools for the analysis of the collected data. The nature and the size of the collected data helped in identifying the most appropriate tools for analysing the data.

The pilot study of this research selected a sample of six individuals from the national healthcare services to participate in the pilot study. This sample covers three main users of electronic patient records. The selected sample includes two ISM personnel, two clinical staff and two non-clinical staff. The outcomes of the pilot study helped to screen the interview design and the clarity of the questions. The outcomes, comments and suggestions of the respondents to the pilot study have been taken into consideration in the next stage of the survey process. The data and interviewee responses collected in the pilot study were analysed in order to ensure that the outcomes reflect the research aims and objectives. The design and the questions of the interviews were updated and edited based on the pilot study responses. Table 3.3 shows the main subjects selected to participate in the pilot study. The table also shows the main drivers and reasons for this selection.

| | Sample | Drives |
|---|---|---|
| Pilot Study | ISM Personnel SA NHS (2) | To help identifying interview design style.<br>To help clarity of the questions, questions wording,<br>To get experience in managing and control of the interview process.<br>To identify and explore technical personnel opinions and views on EPR.<br>Their jobs include implementation and maintenance of the EPR system. |
| | Clinical Staff SA NHS (2) | To help identifying interview design style.<br>To help clarity of the questions, question wording,<br>To get experience in managing and control of the interviews process.<br>Their job role and responsibilities require direct patient care and use of EPR |
| | Non-clinical Staff SA NHS (2) | To help identifying interview design style.<br>To help clarity of the questions, questions wording,<br>To get experience in managing and control of the interviews process.<br>Their jobs require access to certain patient information. |

**Table 3-3 : Pilot study sample and main drives for the selection**

## 3.7 Collected Data Analysis

This work package involves a critical analysis of the collected data and the models. The data analysis includes three main tasks. These tasks include the collected data from the SA NHS, policy consistency of data, conformance of behaviour in model and strategy and solutions. This can be achieved by interpreting the collected qualitative data and identifying its consistency. The qualitative data was collected from different resources within the SA NHS. The main collected data was from the one-to-one in-depth interviews with key experienced subjects working in the SA NHS. The interview, as a tool in collecting data, selected to explore the subjects' knowledge, experience, opinions and attitudes towards the health information services security and particularly to the electronic patient record design and contents of the record.

The collected data is based on the main issues explored in the interviews and are the main streams of the research aim and objectives. The collected data is also used in developing and designing the electronic patient record and health information security models. The outcomes of the one-to-one in-depth interviews analysis have helped in identifying EPR items that needed to be included in the EPR design development. The identified items are based on the participants' responses and views, their job role and responsibilities within the health services.

The proposed EPR model will be evaluated by a second fieldwork survey. The collected evaluation data will be used to identify the agreement between the proposed model and the reality of the NHS. The developed model and the outcomes of the data

analysis will be used to answer Research Question 5, "Is the security policy translated into organisational reality".

## 3.8 Data Collection: for Evaluating EPR Model

Evaluation of a programme or social behaviour is an important part of decision making and system adoption. There is no generic and accepted single definition of evaluation. Most of the definition approaches reflect the author's or the organisation's purpose of the definition. Daniel et al. (2007) introduce and discuss evaluation theory, models and applications. The most appropriate definition and understanding of evaluation is stated as "*assessing achievement against behavioural objectives*". This definition reflects social programme evaluation. The definition needs to identify the social programme achievement earlier against the actual behavioural objectives. The authors also provide a definition that reflects the need for decision making regarding the programme or the system based on the information provided. The definition stated "*evaluation is the collection and analysis of quality information for decision makers*".

A structured questionnaire was used in the evaluation process. The main justification for using a questionnaire in the evaluation process is that a relatively large number of SA-NHS staff can be used in the evaluation process. This increases the reliability of the evaluation outcomes. The other important reason for selecting the questionnaire was convenience and cost. From a process management viewpoint, the questionnaire was manageable and can be achieved in a reasonable time and at a reasonable cost.

The questionnaire was distributed after introducing and explaining the aim and objectives of the research. The respondents were given the right to withdraw from the survey at any time without obligation.

### 3.8.1 Evaluation Samples

It is important and critical to select appropriate subjects for evaluating the developed and designed EPR to ensure its usefulness, practicality and reliability. The evaluation process selected sample subjects need to be experienced and knowledgeable who use EPR as part of their job activities to help in providing constructive comments and suggestions. Two key experienced and knowledgeable subjects from each medical and non-medical staff included in the proposed EPR design matrix were selected to participate in the evaluation process. Table 3.4 shows the sample size for each discipline. The total number of the sample is 46 of the hospital staff subjects

| EPR Evaluation Participants Sample | | |
|---|---|---|
| | Discipline | Sample Size |
| **1** | Consultant | 2 |
| **2** | Registrar | 3 |
| **2** | Physician-in charge of the patient-Resident | 4 |
| **3** | Anaesthetist | 3 |
| **4** | Medical Student | 3 |
| **6** | Nurse | 4 |
| **6** | Matron | 2 |
| **7** | Pharmacists | 3 |
| **8** | Medical lab Technician | 2 |
| **5** | Radiologist | 2 |
| **5** | Research/Development Coordinator | 2 |
| **9** | Senior Manager | 2 |
| **9** | Head of Department | 2 |
| **10** | MIS Members | 3 |
| **11** | NHS Regulatory (Audit) | 1 |
| **12** | Administrator | 4 |
| **13** | Receptionist | 4 |
| | **Total** | 46 |

**Table 3-4 : EPR evaluation sample**

### 3.8.2 Analysis of the Evaluation Data

The collected quantitative data of the EPR evaluation will be analysed using SPSS. SPSS is a well established software for analysing quantitative data. SPSS has been selected due to the nature of the collected quantitative data from the questionnaire responses and because of the statistical analysis tools and methods available in SPSS.

### 3.8.3 Pilot Study: Evaluating Access to EPR Questionnaire

One of the approaches used to ensure that the distributed questionnaire is accurate and reflects the purpose of the design and the contents is to carry out a pilot study. The pilot study helps save time and effort. In this research, the developed and designed

questionnaire for EPR was piloted before distribution to a selected pilot study sample. One of the main purposes of the pilot study is to check the questionnaire wording. The questionnaire questions wording needs to be clear and make sense for the respondents in order to ensure appropriate answers and to check the appropriateness of the questionnaire design. The other important benefit of the pilot study is to check the outcomes of the response analysis. This needs to ensure that the responses serve the research aims and outcomes and the intended outcomes of the questionnaire questions (Creswell, 2003).

Six EPR users were selected to participate in piloting the evaluation questionnaire (see Table 4.4). The total number of participants selected is six: two from each discipline selected, namely two medical doctors, two medical nurses, and two ICT personnel. The participants were selected randomly from the hospital staff, taking into consideration the group's professions, i.e. two participants from each group. The questionnaire was distributed in person in a small quiet rest area in the hospital. The pilot study was managed by the researcher in order to clarify any issues arising. The room was in a quiet area to ensure that there would not be any disturbance to the participants' concentration. The pilot study was carried out at a date and time appropriate for the participants. The hospital management helped in arranging the date and time. The date and time was scheduled during the staff's free time.

A brief introduction to the aims and objectives of the research and the evaluating access to electronic patient record questionnaire was given to the participants as part of the evaluation process. The introduction also stressed the confidentiality of the participants' responses. The introduction also gave the participants the opportunity to ask any questions.

Table 3.5 shows the pilot sample and the main reasons and justifications for the selection. The size of the sample is relatively small. This is mainly due to the fact that the hospital staff are very busy and they have very little free time to participate in such a pilot study. The second reason for the small size is that is was easy to manage in a very busy public service place. The small size also helped in providing almost one-to-one feedback after completion of the questionnaire.

| | Sample | Reasons for selection |
|---|---|---|
| **EPR Evaluation Questionnaire Pilot Study** | Medical Doctors (Residents) (2) | They are the main users of the EPR and play an important role in patient diagnosing and treatments. |
| | Nurse (2) | They participate in patient care processes such as monitoring patient conditions and recording patient developments such as blood pressure, heartbeat and diabetes level. |
| | ICT Personnel (2) | They represent the non-medical staff of the hospital. They are also involved in implementing, updating and dealing with any problem of the information systems of the hospital. |
| **Total** | 6 | |

**Table 3-5 : : EPR Evaluation questionnaire pilot study sample**

### 3.8.4 Main Outcomes of the Pilot Study

The pilot study responses showed no major problem in the questionnaire design and structure. The main feedback of the evaluation questionnaire can be summarised in the following:

1. **Add registrar to the medical survey sample:** The pilot study revealed the need to add the registrars to the medical staff sample. They indicated that the registrars are one of the senior medical staff and their opinions and views on the EPR items and access is important and critical as they are one of the main EPR users. The questionnaire was edited to include the registrar in the hospital staff.
2. **Add Matron, senior nurse, to the medical staff sample:** One of the comments of the pilot study participants is the list of the hospital staff selected for the survey omits the matron or senior nurse. The participants indicated that the senior nurse has an important role in the patient care process and is one of the main users of the electronic patient record based on her job and role in the patient's care process.
3. **Question 3, item 1 should read first kin full name:** The question was not clear for the respondents. The discussions followed the responses; the respondents

indicated that the question needs to be changed to be more readable and understandable. The wording has been changed and checked with the respondents to ensure that the question is understandable and clear for them.

4. **Question 4, item 5 should read 'date of appointment':** Item 5 of question 4 was also identified by the respondents as one of the questions that needed to be modified to become more readable and understandable. The question was changed to ensure that it is clear and understandable for the respondents. The analysis also indicated that the outcomes of the responses reflect the intended reasons for the questionnaire questions. SPSS has been used to analyse the pilot study responses to check the responses and the analysis serves the main aim of designing and developing the questionnaire. The analysis indicated that the outcomes serve the purpose of designing the questionnaire. However, the pilot study helped in understanding and gaining experience in using SPSS. This is mainly in how to use the questionnaire variables and select the most appropriate statistical analysis that serves the purpose of the questionnaire. The analysis identified some similarity in the questions and responses. This has been eliminated in the final version of the questionnaire.

## 3.9 Summary

The chapter presented and discussed justifications for adopting data collection methods, research samples and the interpretative approach as a tool for the research inquiry.

The interpretative approach is the most appropriate means for investigating information systems security policy in national health services. Semi-structured interviews with stakeholders who have a direct or indirect role in the information system security of the national health services have been chosen as the main tool for collecting data. The collected data presents rich sets of information that reflect the key stakeholder subjects' perception, opinions and future vison of EPR and information security policy within the SA NHS. This type of data represents the true reality of the situation of the EPR and the information security systems in the organisation. A critical analysis of the data helps in developing more appropriate EPR and exploring EPR security policy issues and provides appropriate recommendations to improve the current situation of the SA NHS.

This chapter also presented the research methodology adopted in this research. The adopted research methodology is based on the nature of the research which mainly involves exploring reality within the Saudi National Health Services hospitals with respect to EPR security and provides a means to improve the situation in healthcare services in Saudi hospitals.

The focus of the chapter was on identifying the main methods to answer the research questions through achieving the research objectives. One of the main objectives of the research is based on investigating the current situation of EPR in SA NHS. To achieve these objectives, several methods were adopted to achieve this objective and provide an answer to the question as to what is the current situation of information security in SA NHS? Critical document analysis of SA NHS at national and organisation levels was included and in-depth face-to-face interviews with key hospital EPR users were conducted to explore and discuss the current situation and impact of the current EPR security policy translation onto the organisation reality. Face-to-face interviews and a critical literature review were used to develop EPR structure and EPR security policy models. Questionnaires were used to evaluate the EPR structure in order to assess its usefulness, reliability and practicality to the SA NHS. The achievement of the research objectives and answers to the research questions were planned through achieving five work packages. These packages are work package 1: Literature survey; work package 2: modelling; work package 3: data collection; work package 4: data analysis; and work package 5: discussions.

# CHAPTER FOUR:

# INTERVIEW ANALYSIS

Objectives

- Analysis of the current KFH EPR.
- Identify and analyse main elements of EPR.
- Analyse the current EPR access control policy
- Analyse EPR users' perception towards EPR confidentiality
- Analyse EPR ownership and staff EPR training

# 4 CHAPTER FOUR: INTERVIEW ANALYSIS

## 4.1 Introduction

This chapter presents and discusses the main outcomes of the interviews that are used in the development of the analysis models in Chapter 6. One of the main aims of this research was to collect in-depth data and information based on semi-structured interviews with main stakeholders of the EPR to provide data and information. King Faisal Hospital, KFH in Riyadh is one of the main and largest hospitals in SA. KFH is using an EPR system as part of its management system. The system is relatively new and the security of EPR has become an important part of the hospital authority's strategic agenda. A series of interviews was carried out in the hospital between March-May 2010 with several EPR stakeholders in order to identify and explore EPR patient records. The interviews were based on a set of semi-structured interviews, (see Appendix 1).

## 4.2 KFH Electronic Patient Record (EPR)

The main focus of the interviews is the electronic patient record (EPR) and its access policy. Therefore, there is a need to identify and explore the King Faisal Hospital's use of EPR at the hospital. This includes whether the hospital stores and processes patient records electronically as part of their patient medical care process in their daily activities. The first interview was carried out with the hospital's ICT department personnel in order to explore the use of EPR within the hospital and the hospital's ICT strategy. The ICT personnel indicated clearly that they have introduced EPR. The hospital bought the system from the American company SAS, as part of a contract with the hospital. The interviewed ICT personnel stressed that the system is installed and used by the hospital staff as part of the hospital strategy to improve hospital performance and the care system within the hospital. One of the ICT personnel stated in this regard:

> "*Yes, the hospital introduced electronic system to improve the hospital performance and saving time and*

> *effort. We currently store and process patient records electronically. The record start from the time patient enters the hospital till he/she leaves the hospital."*
> (Interviewee 10, ICT Administrator)

The KFH medical staff use of EPR needs to be identified and confirmed to establish effective use of EPR and its related policy. The interviews confirmed the ICT administrator's statement that the hospital medical staff are using the EPR and it is part of the hospital information system. This confirmation came from the hospital medical staff, including the hospital consultants, medical doctors, physicians, and the hospital nurses. The statements stressed that the medical staff use the EPR as part of their patient medical recording process. This has been confirmed by several statements by the hospital medical staff. One of the medical doctors, a physician, stated:

> "*Most of our patient medical record carried out electronically. It is quiet useful and saves a lot of time and effort."* (Interviewee 2, Physician)

The hospital non-medical staff, such the hospital administrators, were also asked regarding the use of the hospital EPR. The non-medical staff also confirmed the use of EPR. One of the non-medical staff, a reception administrator, stated regarding the use of the EPR:

> "*Yes, I do use the EPR, The first contact of the patient with the hospital is through us in the medical reception area. Patient personal details are taking and stored in the EPR*" (Interviewee 8, Hospital Administrator)

### 4.2.1 EPR Structure: Patient's Identity and Medical Information

Medical information record security depends highly on the type of information of the records, i.e. its sensitivity. Sensitivity of the information records and security depend on its impact on the information owner from a personal and ethical point of view as well as on the organization's image and from the regulatory point of view.

The main EPR related questions raised with interviewees were "What are the information elements of the EPR you use?" and "Are there any items you think should not be stored in an EPR? Could you please give your reason for this?". The main purpose of the questions is to identify types of information that need to be included in the EPR. The responses varied depending largely on the role and responsibility of the EPR user. One of the main elements of the EPR explored by the interviewees was patient personal details. They argued that this is needed as a key ID for a patient during his/her medical process in the hospital. They argued that the EPR record should include the patient's full name (patient forename, father name and surname), date of birth, home address, telephone number and first kin. They stressed that this information needs to be in the first section of the EPR and this information can be used as a patient ID. A hospital administrator commented on the EPR element by stating:

> "One of my main job role and responsibility is filling patient personal details in the EPR. This includes patient full name (first name, father name, grandfather name and surname), date of birth, address and first kin." (Interviewee 8, Hospital Administrator)

One of the hospital administrators, after a short pause for thought, responded to the question "Are there any items you think should not be stored in an EPR?" by stating "the patient's photograph". The administrator argued strongly for the patient photo to be included in the EPR in order to facilitate identification of the patient on arrival to the hospital. The administrator interviewee provided two main reasons for including a patient's photo on response to justify his argument. The first and most important reason, based on the interviewee's opinion, is patient identification. The interviewee explained that there are several occasions in which patients used other patients' personal details and names to enter hospital services in order to use the hospital's care facilities. The common cases for using patient names come from people looking for a sick note, for example. The other second important reason for including the photo is to facilitate the patient healthcare process by identifying the patient quickly in health care process and management. One of the administrators stated regarding use of the patient's photo:

> "*I could say without hesitation is the patient photo. We have to have patient photo to facilitate our work. We need justification, I can list you several reasons but my personal experience and the main one is to avoid fraud. There are several occasions patient using different name to get sick note. … in my view, the photo is also helps in facilitating the patient health care process through easier to identify the patient by his/her photo*"
> (Interviewee 9, Administrator)

### 4.2.2 EPR Structure: Patient's Non-Medical Information

Patient nationality was explored by both administrator interviewees. They stressed the importance and the need to include the patient's nationality in the EPR. They argued that the SA NHS has a large number of non-national patients. They are employed by various employers on different contracts and under different medical insurance policies. They also strongly argued including the nationality to help in the patient healthcare process by identifying patients' cultural background, medical history, nutrients, and to help to identify their health insurance contracts. Further, it would help any NHS statistical analysis that may be needed in the NHS plan. One of the hospital managers stated regarding adding the patient nationality in the EPR:

> "*There is a large number of non-Saudi in the Saudi labour market. They have different insurance types and coming from different countries. There is a need to identify the patient nationality to help in identifying the insurance policy and identifying the country in case of death. It is also important to stress identifying nationality of patients helps identifying patient background, previous nutrients, medical history and in statistical analysis of NHS plan and performance*"
> (Interview 1, Hospital Manager)

SA NHS is a large service with a large number of hospitals under NHS management. It is a public service and there is a need for communication and identification of the hospital and the patient national health services. It is no surprise when the hospital manager stressed the importance of identifying the hospital that provides patient care in the EPR. He stressed identifying a hospital on the EPR helps locating patient, locating medical staff providing the care service, helps in hospital and national health statistical analysis in the hospital and national survey.

> "*In our daily work, we have several communications with the Health Ministry and with other hospitals regarding patients in our patient in several occasions that enquire is not sure which hospital is the patient. A database with hospital code in the EPR helps to facilitate communications with various patients' stockholders and facilitating patient health care"*
> (Interview 1, Hospital Manager)

One of the main issues regarding the health services in Saudi Arabia stressed in the interview with the hospital manager is a lack of NHS number for its citizens. Currently, each hospital has its own patient NHS number, based on the hospital patient record file. It emerged from the interview that there was an important need for the Saudi Arabia Health Ministry to provide NHS numbers for its citizens in order to facilitate the NHS management and to improve the quality of NHS services. The hospital manager interviewee argued strongly in favour of patient NHS numbers being included in any responses and in favour of corresponding with other NHS organizations based on this number. The number should be included in the EPR with a patient reference code. The hospital manager stated in this matter:

> "*One of the main challenges in patient's management in SA NHS management is patients care management, monitoring patient's health care and appropriate plan for the NHS. I personally strongly believe there is a need for NHS number for each SA citizens"*.
> (Interview 1, Hospital Manager)

The hospital nurses' interviewees stated that the patient's religion needs to be stated in the EPR due to its importance in supporting patients morally and in taking the right action in case of a patient's death. They described several occasions on the death of patient in which there was a need to take certain actions based on the patient's religion so as to respect the patient and his/her family's religious beliefs.

> "*Patient religion needs to be stated in the EPR to help in respecting the patient belief and to help him/her in practicing his religions … The most important is also the needs to take the right actions on case the patient death"* (Interview 6, Hospital Nurse).

In response to the question 'Are there any items you think should be stored in an EPR that are currently not present? Could you please give your reasons for this?' one of the elements explored by the ICT administrator and the physicians was the need to add some of the clinical tests. They stressed that there are several medical tests which are not included in the current EPR format. One of the physicians stated:

> "*The patient electronic records are still in the process of development. There are several items need to be added to the electronic record such as the clinical testing. The hospital is still using paper based recording system"* (Interview 3, Physician).

The hospital doctors, medical doctors, stressed the need to include the local doctor or GP. They argued that the name of a patient's GP is needed to help in the patient medical process in case consultation with the GP is needed. This is important as SA is a relatively large country with a limited number of hospitals; the main hospitals are mainly in the main cities. Therefore, the local GP's name, local surgery name, address and telephone are important and need to be included.

> "*There is a need to collect medical information as much as we can before preceding the medical process in the hospital. There is a need to interact with*

> *previous patient medical providers for consultation and getting more information when it is required. Therefore, strongly believe the EPR needs to stated the local doctor name, the local surgery name, address and telephone number"* (Interview 2, Physician).

## 4.3 EPR Access Control

One of the main focuses of this research is EPR access control policy. Access control policy issues were explored in all of the interviews and discussed in some detail. The main aim was to identify Who, What and How to access EPR. The interviews indicated that the hospital medical and non-medical staff have access to the EPR. The EPR access differs from one staff member to another depending on his or her role and responsibility. The interviews indicated that the information department staff of the hospital has no restriction in accessing EPR. The main explanation provided for accessing EPR was ICT staff role and responsibility. One of the ICT administrators stated:

> "*I have the right to access patient records; in fact there is no restriction on my team on the access rights".*
> (Interview 11, ICT administrator)

The ICT administrator has challenged by stating that their job does not require accessing EPR. The explanation provided was purely due to lack of clear policy and guidelines on access control to restrict their access. It also emerged that their ICT skills and lack of other ICT skills and awareness made their access to EPR untraceable and open. The ICT administrator also indicated and agreed that there is no need for them to access EPR. They expressed that there is no need for such access. EPR is not related to their job role and responsibilities.

The hospital physicians also have no restriction in accessing the EPR. It was clear all the physicians have given permission to access their patients' EPR. It is part of the physician's responsibilities as one of the physicians stated:

> "*I have no restriction in accessing EPR. In fact I am using the access to EPR as part of my job responsibilities in the hospital. I believe and understand that all the hospital physicians have access to the EPR"* (Interview 2, Physician).

On the other hand medical staff such as most of the hospital nurses has no full access to the EPR. The nurse interviewees explained that most of the nurses do not have full access to the EPR. They stated that most of their work is carried out manually; using the traditional paper based recording forms. The nurses believed that the main reasons behind this denial of full access to most of the nurses are lack of clear policy and the technical skill to design the access control. One of the nurses stated:

> "*I have right to access EPR but not in full. I believe, the hospital is still has no technical and policy for EPR access control"* (Interview 6, Hospital nurse).

The medical staff can be classified into two main groups for accessing EPR. The first group is the physicians, medical consultants who have open access to EPR. On the other hand, most of the nurses and the patients of the hospital were denied full access to EPR.

The nurses explored parts of the EPR record that would need to be accessed by them and why they need to access them. The nurses indicated clearly that they need to access patients' personal details. They explained that patients' personal details such as patient ID were needed as there is a large number of patients in the hospital and they do need to ensure that the right patient is in the right medical care process. They also indicated their need to access some of the patient's medical history such as his/her allergies. They explained that this is needed so as to prevent any action by the nurses from affecting the patient's medical care. Finally, they explained that they also need the patient's current diagnosis. This helps the nurse to manage aspects such as the patient's movement, medicine, and to observe his/her temperature and blood pressure. One of the nurses stated:

> "*Nurse needs to access patent's personal details to ensure she is dealing with the right patient and not mixing up with other patient, patient allergies and current diagnosis as examples"* (Interview 7, Hospital nurse).

The interviews indicated that the hospital patients have no access to their patient record. The explanation given was twofold. Firstly, this is due to a lack of awareness and understanding of the patient's right to access his/her medical records. Secondly, it is due to the lack of policy, process and technical skills to manage patients' access to their medical records. The medical staff, particularly the physicians and consultant, strongly agreed and were in favour of patient access to their medical records. They expressed strongly the patient's right and that the hospital needed to respect this right by allowing the patient to access his or her medical records. They expressed that they are informing the patient's orally about their medical records. The patient's access rights will help patients understand and be aware of their medical record.

> "*The patient has full right to their medical record and I strongly recommend establishing a process for the patient to access their medical record. In fact, it is part of the medical care process to inform the patient about his medical condition, medicine and allergies"*
> Interview (2, Physician).

Patient access to EPR was explored and discussed with ICT Administrators. They indicated clearly that the current policy and procedures used do not give permission to patients to access and read their own personal EPR. However, they pointed out that the patient's access right to his/her own EPR will be granted in the near future.

> "*At the moment, the patient has no access right to their records. It is possible introduced in near future"*
> (Interview 10, ICT Administrator).

The interview indicated that the hospital manager is not quite aware of the importance of the patient's access right to read their own personal medical record. The manager believed that the medical doctor provides the patient with the necessary medical record and therefore, there is no need to complicate the access system. One of the hospital managers expressed this view by stating:

> "*The patient has enough information to their medical record through their medical doctor. They provide the patient regarding their medical conditions and the medicines need to be take"*
> (Interview 1, Hospital Manager).

The interviewees were asked whether they have consent from the patient to access their own EPR. The interviewees' indicated different opinions towards the owner of the medical information and the need for patient consent. There are people within the hospital who indicated that the EPR owner is the hospital and not the patient. Therefore, there is no need to take a patient's consent in order to access the EPR. However, they agreed that this information should not be passed to a third party without the patient's consent. The hospital manager commented regarding this issue:

> "*There is no need to take patient consent for accessing EPR. The data and information created by the hospital and the EPR ownership must be kept within the hospital"* (Interview 1, Hospital Manager).

The interviews and the above statement indicated that the hospital's current policy does not regard the patient's consent as part of the requirements for accessing EPR. They believed that the hospital and not the patient owns the EPR.
The main method used to access EPR is based on using a username and password. Each EPR user is provided with a username and password through an access permission application form. The application form needs to be signed and declared by the hospital authority and ICT department. The access permission is controlled by two departments.

The first is the hospital authority, hospital manager, and the ICT department. The ICT department looks after setting the access control while the hospital management sets the access permissions. One of the ICT administrators stated:

> "*The medical record users need a user name and passwords to enter the system. This is usually set by the medical record department at the hospital custodians"* (Interview 9, ICT administrator).

The interviewees indicated that there is no way that the EPR can be accessed apart from using the username and the password provided. They indicated that the IS system is designed based on certain rules. These rules are very difficult to be broken by a third party. They believed that the design is well secured and there is no chance to break the system.

The current information control is in the hands of two groups. The first group is the hospital management. They decide the access rights for the hospital staff based on their role and responsibilities. The second is the ICT department who set the access. The hospital has very strict rules as no one has the right to pass his/her own access right privileges to a third party, whether internal or external users. The interviews indicated positive attitudes towards this issue as the vast majority of the interviewees stressed that the passing of access rights to another person is against the rules of the hospital. This meant that the staff have an understanding and awareness of the current access control policy.

Editing EPR is one of the main focuses of the interviews. The interviewees were asked about their ability to modify and change EPR. It was clear from the interviews that hospital physicians and consultants are able to add new medical information to the EPR. The physicians also stated that they do not have the ability to delete already existing information. They stressed that there is a clear restriction in deleting or moving information from the EPR.

The administrator interviewees indicated that they are able to change the patient's personal details such as a change in his/her address or telephone number. The

administrators also indicated that there is a restriction in changing or deleting any currently existing information on the EPR. Surprisingly, the ICT administrator indicated that the current system has given permission to change the EPR. One of the ICT administrators stated:

> "*I have the ability to change and modify the EPR but it is not part of my job role and responsibility. This is purely based on my ICT role and rights to access the IS. There is no restriction on my access right"* (Interview 11, ICT Administrator).

The medical staff indicated that the current EPR form needs to be modified and needs to be made easier. They indicated that the current form is not a user-friendly document. They indicated that EPR entries need to be modified:

> *"The current EPR design needs to be changed to make it more easy to use and clearer. I found it difficult to navigate and search for information for patient with long medical history"* (Interview 2, Physician).

The technical department, through the ICT administrator, explored the hospital staff training needs. They indicated that one of the main challenges of their daily activities is the staff's ICT skills and competence. They explained that the majority of their daily activities is spent helping and supporting effective access and use of electronic information.

> "*One of the main challenges of EPR access is the hospital users skills and competence. The vast majority of our daily jobs is helping and supporting staff accessing and use of EPR effectively"* (Interviewee 10, ICT administrator).

The pharmacist clearly indicated that the hospital pharmacist has read access rights to the EPR. It argued that this access right is based on the pharmacist's role and responsibilities in the patient care process. The pharmacist stated:

> "*I have read access to certain part of EPR, of course to reflect my role in the patient care process. I need to ensure the right medicine to the right patient without any errors"* (Interviewee 13, Pharmacist).

Table 4.1 shows hospital access rights for reading and writing to the EPR based on the interviews' main outcomes. The table classified access to the EPR into three main access categories. The first category has an open access right to the EPR without any restriction. This category includes hospital managers (hospital authority), senior medical staff, such as physician and consultant and ICT administrator. The second group has partial access control rights to certain elements of EPR. This group includes administrators, nurses, and pharmacists. The administrator has read and write access to the patient's personal details only while the pharmacist has read access only. Some nurses have been given partial access to EPR. This is mainly due to their job role and responsibilities. On the other hand, the patient is denied access to his/her own EPR.

**Table 4-1 : KFH EPR access right**

| | Interviewed Subject | Access | Type of Access |
|---|---|---|---|
| **1** | Hospital Manger | Open | R/W |
| **2** | Medical Doctors | Open | R/W |
| **3** | Consultants | Open | R/W |
| **4** | MIS Members (ICT Admin.) | Open | R/W |
| **5** | Nurses | Partially | R/W -Partially |
| **6** | Pharmacists | Partially | R only |
| **7** | Administrator | Partially | Partially R/W |

## 4.4 EPR Access Control Policy

Information security policy was explored in the interviews, aiming to establish whether the hospital has a clear policy and to identify any gap in the policy. The interviewees believed that the hospital has an information security policy but that it is generic and not EPR-specific. They stressed that all the hospital staff are given a copy of the hospital's security policy. However, the physician stressed the need to improve and update the current policy due to changes in patients' rights and to avoid any unauthorized access to the EPR. One of the physicians stated:

> "*The hospital has certain rules and procedures for security policy. I have been given the document but I believe the document need improvement and updating to reflect the recent changes in patient rights"* (Interviewee 3, Physician).

The main concern of the current security policy is generic and does not reflect the hospital and information security needs. One of the physicians interviewed, Interviewee 3, commented on the current policy as:

> "*Policy copied from other hospital policy without taking in consideration the cultural and the hospital current activities"* (Interviewee 3, Physician).

The policy is written and enforced by hospital senior management. They are responsible for establishing and implementing the security policy. It is part of their role and responsibilities. However, they take advice and consultation from other departments, and particularly the ICT department.

> "*Senior management, the hospital authority, is responsible for the hospital policies and strategy. One of these responsibilities is the policy towards EPR security"* (Interviewee 3, Physician).

The security policy clarification is subjective and depends on the type of enquiry. In each profession or department there is a trained individual on the system and security policy. Usually, the staff refer to this individual. In case individual clarification is not enough, staff are referred to the senior management as they are the main decision makers in security policy, due to the hospital's management structure and responsibility.

Access control is determined in the hospital based on two factors. The first factor is the individual staff role and responsibilities within the hospital. The second depends on the ICT department access setting process and the ability to set such access. The hospital access policy is based on job specifications. Each individual staff has a set of job

specifications set at the recruitment stage. However, a head of department has the right to add more, within reason, and to ask senior management to modify the role.

> "*My access is mainly controlled by senior management based on my job rules. Medical record department particularly is the one who set my access rights"*
> (Interviewee 2, Physician).

The main body to determine access control is hospital senior management. The main reason is the management style whereby senior management is the source of decision making. The senior management is in control all hospital activities with minimum opportunity given to others to lead in their workplace.

There are several security risks in implementing EPR strategy. There are several risks explored in the interviews. One of the common risks is that an EPR user may leave the record open and go on to something else, forgetting to log out or to close the record. This allows an unauthorized person to access the EPR. There were also several occasions on which there was a problem in accessing and navigating the system. The problem could be a virus or an intruder to the system. The process used to address such risks was mainly through the ICT department with the help and support of the medical records department. The head of each department was also aware of such a risk. They were informed and encouraged to introduce and implement security policy in their department strictly and firmly so as to avoid any misuse of the electronic patient record. One of the physicians stated:

> "*Medical record department is addressing any security issues and deal with it accordingly. However, there is no clear policy and or strategy on security policy"*
> (Interviewee 3, Physician).

## 4.5 EPR Users' Confidentiality Perceived

One of the main challenges of EPR security is the medical and medical staff confidentiality perceived. This plays an important role in the EPR information protection and security due to the interaction between the IS department and the staff.

The interviews indicated that hospital are aware of and understand the confidentiality of the EPR. They identified several items within the EPR as confidential items. Generally, the medical staff focused on the medical elements of the EPR as critical and confidential, such as the illness, length of the illness and the current medication. This reflects their role in the patient medical care process. On the other hand, the non medical staff focused on the patient's personal details such as the patient's address, home telephone number and mobile number. Table 4.2 shows the EPR confidentiality staff perceived. The table clearly indicated that the hospital staff has positive attitudes regarding EPR confidentiality.

**Table 4-2 : EPR confidentiality staff perceived**

| | Interviewed Subject | EPR Confidentiality perceived | Subject Response |
|---|---|---|---|
| **1** | Hospital Manager | √ | "*EPR is one of the important confidential documents in the hospital. We have clear policy to ensure its confidentiality*." (Interviewee 1) |
| **2** | Physicians | √ | "*Patient medical condition, diagnosis, critical needs to be kept confidential and should not be accessed by anyone apart from the patient medical physician without the patient consent*".( Interviewee 3) |
| **3** | Consultants | √ | "*The EPR is critical confidential document and the hospital should take all the measures to ensure its confidentiality*.", (Interviewee 5) |
| **4** | MIS Members (ICT Admin.) | √ | "*I believe, there are several items within the EPR are confidential information such as the patient personal details, medical tests result and diagnose*." |
| **5** | Nurses | √ | "*I highly rate the EPR confidentiality. The medical part of the record should only accessed by the hospital medical staff*.", (Interviewee 6) |
| **6** | Pharmacists | √ | "*Patient medical history. Patient condition and patient medication*" (Interviewee 12) |
| **7** | Administrator | √ | "*No doubt in my mind, the most critical information on EPR is the patient personal details, especially the patient mob number as we had a problem regarding patient mob no*," (Interviewee 9) |

### 4.5.1 EPR User Training

The EPR system used in the hospital is based on an American system called SAS. The hospital trained a group of hospital staff in America in the system. The hospital strategy selected one staff member from each profession in the hospital to be trained in the system. The trained group included a physician, nurse, administrator, consultant, ICT administrator and hospital manager. One of the senior managers justified and explained the selection process strategy by focusing on the trainees' role after training. He explained that the plan was that each individual trained in the States would be responsible for the system training activities in his/her department and would be responsible for any enquires within the department. He stressed that the strategy worked very well. He also explained that the management also provided and facilitated a link with the company in case of any enquiries from the trained staff regarding the system.

The interviewees confirmed that one of the main parts of the USA training is EPR confidentiality and protection. Several scenarios to enhance and promote EPR protection and confidentiality were presented and discussed. The training also discussed the consequences and possibilities of internal threats to the EPR security from internal and external users. The security and protection threats were discussed and focused into two main tiers. The training was based on USA scenarios, use of technology in protecting the EPR, and based mainly on the trainer's experience. The first tier is based on technology threat and the second tier is based on human factors. The human tier is based on individual staff behaviour, attitudes and culture. Individual staff may release or pass information to a third party without awareness of the consequences of such an act. This may be related to the individual culture and organization culture towards EPR confidentiality,

> "*I have been on a medical training programme in USA. One of the training elements is the medical electronic protection"* (Interviewee 10, ICT administrator).

Table 4.3 shows EPR confidentiality staff training. The table shows the KFH staff and the state of training and comments regarding his/her training

**Table 4-3 : KFH EPR training**

| | Interviewed Subject | Trained | Comments |
|---|---|---|---|
| **1** | Hospital manager | √ | Has brief training on the system |
| **2** | Physicians | √ | Both physicians went to USA in training course in the system |
| **3** | Consultants | √ | One consultant has one-to-one training course and other went to USA for training in the system |
| **4** | MIS Members (ICT Admin.) | √ | One of the ICT has formal in-house training course and other went to USA for training in the system |
| **5** | Nurses | √ | One of the interviewed nurse trained with external training provider in USA, Interviewee 7, and the second trained in-house training, interviewee 6. |
| **6** | Pharmacists | √ | Pharmacist has a brief introductory to the SAS system without formal training. |
| **7** | Administrator | √ | Both administrators interviewed attended in-house training on the system. |

The other important point explored in the interview is that the induction programme for new recruits does not include the importance of the EPR information security, scenarios and practical examples. This issue has been explored by one of the interviewees.

> "*Induction programme for new recruit need to include importance and seriousness of the EPR information security with practical scenario and examples"*
> (Interviewee 2, Physician).

### 4.5.2 Patient Rights

The patient rights issues explored in the interviews aimed to (i) identify hospital awareness, attitudes and opinions towards patient rights and (ii) to explore the current practice and procedure enhancing patient rights. The interviewees clearly agreed with the patients' right to access their own EPR records. Most of the interviewees statements showed a strong belief in the patient rights. However, the patient and consultants users of the patient EPR were stronger believers in the patient rights than

other users such as hospital nurses, technicians and the management. It can be argued that this is due to their awareness, experience and knowledge of the patient rights in the West. One of the physicians stated:

> "*The patient has full right to their medical record and I am strongly to establish a process for the patient to access their medical record. In fact, it is part of the medical care process to inform the patient about his medical condition, medicine and allergies"*
> (Interviewee 2, Physician)

From a practice point of view, the hospital has no rules, policy or clear guidelines regarding patient rights. Some physicians give their patients the right to access their own EPR. One of the physicians, when asked about the patient's right to access his/her own EPR, confidently stated that the patient has the right to access his/her own EPR. He stated:

> "*Yes, I always give the patient full access to his/her information at the patient convenient time. I have no any restriction to any information. As I told you earlier, the patient is sole owner of the EPR"*
> (Interviewee 3, Physician).

However, the physician explained that this was a personal practice based on his personal belief in the importance of patient awareness and understanding of his/her medical case. The hospital has fallen short in clarifying the patients' right to access his/her own record. There is no clear policy and guidelines regarding the patients' right. One of the nurse stated :

> "*I am aware and believe in patient right. The EPR is purely their personal medical information. From my part on the patient right process, I have guidelines to follow regarding the patient right"* (Interviewee 6, Hospital Nurse).

One of the critically important issues explored in the interviews is that the SA NHS does not have any process or forms for patient consent. Patients' records are transferred within the SA NHS and with EPR stakeholders without patients' permission. One of the interviewees stated:

> "*Currently there is no any process or forms for patient consent. The patient's record transferred to different stakeholders without patient consent. This is not right in my view"* (Interviewee 1, Physician).

One consultant responded to the patient right policy within the hospital practices. He responded by assuring the need for clear policy and guidelines regarding patient rights and stated:

> "*We are on the early stage of establishing clear policy regarding the patient right compared with developed country. However, we are in the right track. We have started several steps towards patient right, such us encouraging staff to brief the patient about his medical case as an example"* (Interviewee 5, Consultant).

## 4.6 EPR Ownership

The EPR ownership was explored in the interviews to identify the interviewees' opinion and perceptions of EPR ownership. There is a diversity in the interviewees' opinions towards EPR ownership. The hospital custodians strongly believed that the hospital owns the EPR. They explained their opinions in two ways. Firstly is the fact that the record was created by paid hospital staff. Therefore, the ownership should also belong to the creator of the record. Secondly, they argued that since the information is medical based information, the owner of such information should always be the hospital. The Hospital Manger was asked about the patient's ownership.

On the other hand, the ICT department claimed EPR ownership. They argued that the EPR is managed, controlled and maintained by the ICT department. They are the

department who set the access to EPR and who develop and implement the medical information systems. One of the ICT administrators stated:

> "*I think the owner of the EPR is the medical information department. They are the main developer and implementer of the medical information system. Therefore, they are the sole owner of the EPR"* (Interviewee 11, ICT administrator).

One of the strongest views toward the hospital ownership of the EPR came from the hospital administrator. The administrator strongly believed that the EPR ownership belongs to the hospital management, arguing that the main right of the patient is to have appropriate and correct medical care.

> "*Of course, the patient is the owner of his/her personal medical record. The hospital role is focused in medical care and the information is purely to help this care"* (Interviewee 9, Hospital Administrator).

The hospital medical consultants have a clear and strong opinion towards patient ownership of their personal medical record. They argued strongly that the role of the hospital is purely on patient care:

> "*Of course, the patient is the owner of his/her personal medical record. The hospital role is focused in medical care and the information is purely to help this care"* (Interviewee 5, Medical consultant).

The hospital nurses do not have clear opinions regarding the EPR ownership. However, they believed that the ownership is between the hospital management and the patient. They divided the EPR document into two parts. These parts are the personal details part and the medical part. The personal details part is believed to belong to the patient while the medical details part belongs to the hospital management. Their argument is based on the fact that the medical information record is created, controlled and maintained by the hospital.

> "*Of course, the patient is the owner of his/her personal medical record. The hospital role is focused in medical care and the information is purely to help this care"* (Interviewee 7, Hospital Nurse).

Table 4.4 shows the outcomes of the interview discussions regarding EPR ownership. It is clear that there is a diversity in opinions toward the EPR ownership. There are three different opinions. The first opinion is the strong belief that the ownership of the EPR belongs to the hospital management. The hospital management and the hospital administrators represent this view. The second opinion focuses on patient ownership. It seems the medical profession, namely the medical hospital staff and the physicians represent this view. The third opinion is that ownership is mixed between the patient and hospital management. These opinions are expressed by the hospital nurses, pharmacists and patients. Only the ICT personnel believed that the ownership should belong to the ICT department.

**Table 4-4 : EPR ownership**

| | Interviewed Subject | EPR Ownership | | | Comments |
|---|---|---|---|---|---|
| | | Hospital | Patient | ICT Dep | |
| **1** | Hospital Manger | √ | × | × | Strongly believed towards hospital ownership |
| **2** | Physicians | √ | × | × | Strongly believed towards patient ownership |
| **3** | Medical Consultants | × | √ | × | Strongly believed towards patient ownership |
| **4** | MIS Members (ICT Admin.) | × | × | √ | Moderately believed towards ICT Department |
| **5** | Nurses | √ | √ | × | Not clear opinions, they believed the ownership is between Patient and hospital |
| **6** | Pharmacists | √ | √ | × | Not clear opinions, they believed the ownership is between Patient and hospital |
| **7** | Administrator | √ | × | × | Strongly believed towards hospital ownership |

## 4.7 Auditing

The interview explored several interviewees who were not aware of any auditing carried out at their department regarding access to the EPR. However, the interviewees expressed the importance and the need for auditing access to the EPR. However, the

ICT interviewees were of the opinion that the hospital has an auditing and quality assurance policy and strategy regarding access to EPR. However, the interviewees were focusing on monitoring and the ability to list the users of the EPR, i.e. their logging on time and tracking any changes to the system. However, they fell short of explaining and providing practice of an independent auditing team to evaluate and audit the access to EPR. This includes any strengths and weaknesses of the current EPR access control policy and suggesting steps to improve the current access control policy. It was clear from the interview that the hospital has a clear quality assurance policy regarding the quality of health. However, the outcomes of the interviews suggest that there is a high level of awareness and understanding towards the importance of EPR editing and logging of any EPR access. One of the interviewees stated:

> "*No doubt, it is critical to our continuous patient health care improvement process to carry out auditing to identify our strengths and areas for improvements. I do believe we need to be robust on out auditing process"* (Interviewee 5, Consultant).

## 4.8 EPR Policy

The interviewees stated that the first step to ensure EPR security is by establishing a clear and appropriate EPR policy. They stated that the policy helps the EPR users' awareness and in understanding the users' EPR roles and responsibility. One of the physicians stressed:

> "*If your interview mainly to discuss EPR within our hospital, the first issue we need to discuss the EPR policy. I do like to stress the first step in adopting EPR system in the hospital is to establish EPR policy without it we cannot move forward regarding the EPR security. …. Clear policy helps us in identifying our roles and responsibilities toward EPR"* (Interviewee 3, Physician).

However, currently the hospital has a certain policy regarding EPR security. The hospital has a security policy document. The document is distributed to the medical staff with respect to the use of ICT within the hospital. The document lacks a clear statement regarding the roles and responsibilities regarding the use of EPR. The current policy document focuses on ICT issues with little focus on the critical electronic medical record such as the EPR. One of the EPR users stated:

> "*There is no clear statement regarding the EPR security. The current policy is generic ICT policy. There is a need for clear policy regarding use of EPR"* (Interviewee 2. Physician).

The hospital currently uses an American EPR system. The system was purchased from and installed by American experts. One of the main issues explored in the interview is that there is a lack of a clear statement on the system's reliability. Some argued that the system provider needs to provide evidence and assurance regarding the reliability of the system they are using. They stressed that the hospital authority fell short of providing evidence and policy to ensure the reliability of using such a system and the EPR is safe from any internal and external intruder. They argued that a reliable and secure system motivates both medical staff and patients to use EPR in the patient medical care process. One of the physicians stated:

> "*The hospital has certain rules and procedures for security policy. I have been given the document but I believe the document needs improvements and updating. There is no clear reliability and security related issues. Sorry, what do you mean by that? Can you explain? There is a lack of statements ensuring the reliability of the system we are using and security. There is a need for guarantee statement from the American supplier of the system and from the hospital ICT department. This is needed to motivate*

> *the medical staff and patients to use the EPR system"*
> (Interviewee 2, Physician).

The EPR policy responsibility declared in the interview is the hospital authority's responsibility. The interviewees stated that the hospital also needs to regularly update the policy to cope with changes and development in the ICT as well as in the internal environment. One of the interviewees stated:

> "*Senior management, the hospital authority, is responsible for the hospital policies and strategy. One of these responsibilities is the policy towards EPR security. What's about if you are not ensure? I usually ask my senior staff for clarification or one of the medical staff such as the senior nurse"*
> (Interviewee 2, Physician).

## 4.9 Security risks arising from the use of EPR

The main risk from use of EPR comes from abusing the use of EPR. Abse of EPR can take three forms. The first is copying the EPR without permission, the second changing the content of the EPR, and the third passing the information to a third party without authorization. The intruder can be from within the hospital, an internal user or an external user. An ICT administrator clearly identifies the intruders by stating:

> "*I am quite aware of the risk associated with un-authorized access to the EPR. The risk can be from internal or external intruders"*
> (Interviewee 11, ICT Administrator).

Another ICT administrator explored the three forms of the risks associated from using EPR. He stated clearly the three forms.

> "*The main threats to the EPR include copying EPR electronically and using the photocopiers available in all hospital departments, possibility removing and changing some content of the EPR and finally passing the information to third party"* (Interviewee 10, ICT Administrator).

One of the questions explored in the interview was "*Are you aware of any security risks arising from the use of EPR?"* The security risks explored in the interviews were focused on the unauthorised access to EPR and abuse of the content of the EPR. The risks explored can be divided into two main risks, human risk and use of technology risk. The first risk was based on human behaviour towards EPR. Several interviewees identified several current cases in which staff had left EPR information on their PC without locking the PC. This behaviour gives intruders access to EPR and represents a serious risk to EPR security. This issue was explained by one of the interviewees who stated:

> "*Several times, during my duty to update IS system, I have found PC on with EPR. The user forgot to logout of the system. This is bad experience"* (Interviewee 10, ICT Administrator).

This issue was also discussed by physicians at the hospital. One of the physicians stated regarding this risk:

> "*From personal experience based on my observation, the main risks arising from use of EPR, I have seen staff forget to log off from their machine after their entries and leaving the EPR opened. This may be opportunity for intruder to access EPR and abuse the system"* (Interviewee 2, Physician).

The above risk mainly represents staff behaviour toward use of EPR. However, this risk is bad practice within the hospital activities and raises the issue of the hospital working culture.

Patient privacy was one of the main concerns of the physicians in the process of shifting from traditional patient medical records to EPR. The concerns were based on the fact that EPR is easier to copy, edit and send than traditional medical recording data due to its nature as electronic data. This puts patient privacy at risk in case of any unauthorized access to the EPR and breach of patient privacy, which is now protected by several national and international regulations. One of the physicians stressed this risk by stating:

> "*The main risk is the possibility of breaching patient privacy. Traditional patient medical record is difficult to transfer, copy and edit. In other hand, the EPR is opposite. Therefore, I stress the main risk of using EPR is the possibility of breaching patient personal and medical information"* (Interviewee 3, Physician).

The risk of such behaviour can lead to intruders using EPR for their own benefits. This may include copying the EPR or adding information. This represents a threat to the patient's medical process. Medical staff also explored this issue as several staff agreed that several colleagues had left their PC on while going to some other activities or leaving for personal reasons. They agreed that this is bad practice and that there is a need to change. One of the consultants expressed the need to change the hospital information culture. He argued that this issue has improved in recent years and that the hospital is in the process of improving its cultural activities by promoting good practice in hospital activities. The other risk is due to lack of technical protection of the EPR. The interviewees expressed the view that a lack of technical protection and security of the hospital IS can lead to access by external intruders. This gives external intruders the opportunity to change the content of the EPR and/or to explore the medical condition of patients. The main worry of the interviewees is the possibility of making EPR public,

especially for well known public figure patients such as the Kingdom's princes, Sheiks or other well-known society figures.

One of the main challenges is the security risk from the use of EPR. This is a critical issue explored and stressed by the interviewees. This is mainly due to the sensitivity of the information:

> "*Medical record department is addressing any security issues and deal with it accordingly. However, there is no clear policy and or strategy on security policy"* (Interviewee 2, Physician).

## 4.10 Summary

Hospital staff and management are aware and understand the importance of and the need for the patients' right to access their EPR. However, senior medical staff were more aware of and understood the patients' rights better than other staff such as nurses and administration staff. However, the hospital appeared to have failed in their commitment to provide policies and guidelines to enhance patient rights.

The main risks arising from the use of EPR come from unauthorised access to EPR from internal and external users. The risks involve three forms of risk. This includes copying the EPR, making changes to the content of the EPR and passing the EPR to a third party. These risks arose from users leaving the PC logged on whilst away from the PC, and from providing permissions that are not based on the individual roles and responsibility in the patients' medical care process.

# CHAPTER FIVE:

# RESEARCH MODELS: EPR AND ISM SECURITY POLICY MODELS

Objectives

- Develop the EPR model for qualitative analysis.
- Develop ISM security policy mode.

# 5 CHAPTER FIVE: RESEARCH MODELS: EPR AND ISM SECURITY POLICY MODELS

This chapter presents and discusses the development of two research models. The first model is the EPR model. The model aims to provide design and detail medical and non-medical information of the patient. The model is needed to analyse security policy translation onto organisation reality. The second model is the IS model, including the EPR access control model. The developed models are evaluated with the Saudi national health services for their validity, practicality and opportunity to be further developed. The evaluation of the models is presented in Chapter 7.

## 5.1 Introduction

The use of patient electronic systems improves the quality of health care services (DesRoches, 2008). The House of Commons Health Committee for The Electronic Patient record (2007), stated that "Detailed Care Record (DCR) systems can bring dramatic improvement to the safety, quality and efficiency of NHS care, not only through faster access or and sharing of patient information." Of course, effective access sharing requires an appropriate and reliable infrastructure. Olola et al. (2011) argued that lack of infrastructure for electronically sharing pertinent patient data impedes sharing of patient data for patient continuity care. This lack Part of the DCR provides patient's record and this stresses the importance and role of the patient's record in the patient's healthcare process. The question within the health services systems remains the satisfaction with the system functionality. DesRoches, et al. (2008) argued that physicians in USA are generally satisfied with the current EPR system. Healthcare services need to identify the exact patient information that needs to be held on the patient electronic records. The main problem of this is the possibility of including more details that are needed for the system and access control. This may be in conflict with patients' interests and rights.

### 5.1.1 EPR Main Elements

The literature survey and the qualitative interviews explored several record elements that need to be included in the EPR. This information was collected and then grouped

based on their types to facilitate designing the EPR security model. As far as the researcher is aware, there is no such detailed structure for the SA healthcare services that has been developed. Figure 5.1 shows proposed electronic patient record main elements based on the patient information types. These elements include patient personal record, patient personal related record, medical history, patient appointment record, patient medication, patient admission record and non clinical record. The patient electronic record needs to be structured based on its purposes and the sensitivity of the information to the users. This is achieved through the designing and modelling of access control policies. A matrix of the proposed EPR is designed to identify the main EPR users and access control for each element of the EPR.

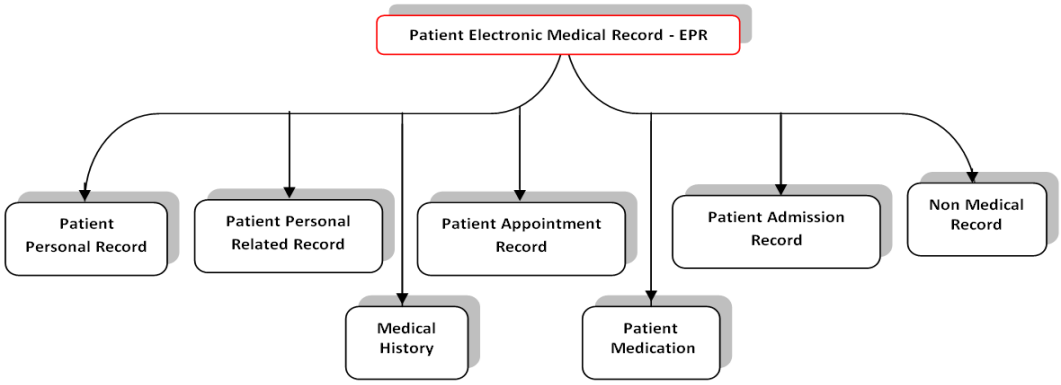



**Figure 5.1: Main Elements of the proposed EPR structure**

### 5.1.2 EPR Matrix

One of the main challenges to EPR is ensuring patient privacy. There are several studies in the area of EPR security (Steele, 2010; Weider , 2007; Sujansky, 2010) but they provide a detailed structure to ensure patient privacy and increase system security. One of the main aims of this research is to develop an EPR matrix for EPR access control and to analyse policies based on the matrix. The matrix is based on two main outcomes. The first is the qualitative data analysis in SA and the second is based on the outcomes of the literature survey (Chapter 2). The main reasons for developing an EPR matrix is summarized in the following table:

**Table 5-1 : The main reasons for developing EPR**

| Reason | Justification 1 | Justification 2 |
|---|---|---|
| **Patient Privacy** | The matrix provides restrictions on accessing and using EPR based on the users' role | The matrix classifies the EPR information based on the sensitivity of the information |
| **Patient Power** | The matrix gives the patient power in controlling his/her information. | The matrix helps the patient to give permission to part/parts on the information by giving consent. |
| **NHS Management** | Helps in developing analysis of access control policy based on the staff role and hierarchy. | Helps in complying with national international regulations regarding patient privacy rights |
| **NHS Culture** | Clear EPR access control helps in building positive NHS culture among staff | Reduce conflicts within NHS hierarchy such as between medical staff such as doctors and management |
| **System** | Helps in system design process | The matrix structure helps in eliminate/reduce any unauthorized users by creating several access, shells, to EPR |

The EPR contains significant information. It is critically important to classify the EPR based on two main factors. The first factor is type of information, sensitivity of the information based on the patient consent. The second factor is based on the EPR users' needs. Based on these two factors, this study developed a matrix to help in controlling the patient privacy based on the above two main factors. The matrix gives the access privilege based on the user's job role and needs and based on the sensitivity of the information, i.e. classifying EPR information.

The matrix was designed to capture users' privilege access to EPR. The access is based on the EPR users' role in the patient care process. The EPR users' role and hierarchy are based on the main outcomes of the qualitative data analysis and the literature survey. The first column of the matrix represents the main EPR users. The column is divided into five main categories and sub-categories.

**+ People: EPR users**

- **P1: Patient**
- **P2: Medical**
  - P21: Consultant-Physician
  - P22: Physician
  - P23: Anesthetist

- P24: Medical Students
- P25: GP

- **P3: Medical Support**
  - P31: Nurse
  - P32: Radiologist
  - P33: Pharmacist
  - P34: Medical Lab Technicians
- **P4: Non medical-NHS Management**
  - P41: NHS Senior Managers
  - P42: MIS Staff
  - P43: NHS Audit Team
- **P5: Non medical-Administration**
  - P51: Administrators
  - P52: Receptionists
  - P53: Law Enforcement

The following sections describe the contents of the EPR main elements and their justifications. The elements are divided based on the type of information and its sensitivity. The contents of the matrix will be used in developing the EPR matrix model that will be used in the analysis of EPR security policy.

### 5.1.3 Patient Personal Record

One of the critical data on patient personal record in the patient health record is the patient's identity. This is due to the large number of patients in the hospital services processes and the possibility of some common personal details. Therefore the patient electronic records need to avoid any mix-up or confusion on the patient record due to the serious impact this could have. Therefore, the patient electronic record needs to consist of several personal detail elements about the patient's identity. This is also security critical because it contains personal details of the patients. Table 5.2 shows the main elements of EPR, patient personal record and this section presents the justification for including each item.

**Patient Hospital Record:** The SA NHS Hospital management system needs a patient ID number and patient hospital record. This is needed for a quick search in the hospital system for patient identity and can be used for statistical analysis in evaluating hospital performance. It is also easier to use a patient code in the patient care process rather than personal details. Patient hospital record is also an excellent approach in ensuring patient personal security. The code can be used in communication and transferring records in the patient health care process. This ID number needs to be at the top of the patient medical record.

**Patient NHS Number:** An NHS number is needed to identify the patient as well as for verifying the patient's eligibility for the health services (The Health Committee, 2007). Each SA citizen has a unique NHS number. Therefore, it is important to use the number in the patient electronic record. The Saudi authority recognizes the importance of the NHS number in the health service sector activity. The Saudi authority has a plan to introduce a new health service scheme whereby the NHS number is a part of the new scheme. The ID number should be a national number while the patient hospital ID number is the hospital reference number.

**Patient Title:** Patient title is added to the electronic patient record for two main reasons based on the interview analysis. The first reason is for identity purposes and the second is the patient's right to be called and identified based on his or her preferred title.

**Patient Surname:** The literature identified patient name as one of the main EPR elements. Individual surnames are the most common forms used to identify individuals. A patient's surname can be helpful in searching the patient's record, identifying him or her in the ward or when calling the patient. The EPR needs to include the surname as the one of the identity elements in the patient personal record.

**Patient First Name:** The patient's first name is needed to identify the patient's identity. It is highly possible to have several patients with the same surname. A patient's first name can be used to identify the patient.

**Patient Photograph:** A patient's photograph has been stated by several authors as an item that needs to be included in the EPR (Sridhar et al., 2009). Interviewees expressed

the opinion that storing patient photographs serves the security process and helps to identify the patient.

**Patient Mother (Maiden) Name:** The patient's mother name has been explored in one interview as an important item that needs to be added to the EPE. The main drivers for including the patient's mother name was stressed as extra patient identity due to the possibility of common names and date of birth. The patient's mother name is used in the SA NHS culture for confirming a patient's identify.

**Date of birth:** Date of birth is one of the main EPR elements identified in the literature and the interviews. A patient's date of birth is needed for two main reasons. The first is an identity and the second for the medical process. The date of birth can be used beside the patient's full name to identify patients. The date of birth is also needed in the health process. The patient's age plays an important role in the health care process.

**Patient Home, Mobile and Work Telephone Number:** Patient telephone contact is included in the EPR. Patient home, mobile and work place telephone numbers are needed mainly for communication purposes. The hospital needs to contact patients and the most effective way of communication, particularly in urgent situations, such as appointment cancellation or a change in the appointment time, is by telephone.

**Gender:** Patient gender is included based on the literature and the interviews. The main reasons for including patient gender are (i) patient identity, (ii) help in taking medical and care decisions.

**Marital Status:** Patient marital status was one of the items that was discussed in the interviews as being needed. Marital status can be used in the patient identification process and helps in contacting the patient's next of kin such as wife, son or daughter.

**Home Address:** A home address is needed to identity the patient and in the correspondence process.

**Religion:** A patient's religion needs to be included, based on the interview, in the patent electronic record due to the importance of the identifying patient record in the patient care process during his/her treatment process. Medical and non-medical staff need this information in the care process. A patient's religion needs to be respected in

the hospital and the hospital staff need to be aware of the patient's religion in case he or she want to practice his/her religion. The second reason is the patient's diet. The hospital needs to identify the patient's religion in order to help them to identify the appropriate diet for the patient. Finally the patient's religion is needed in case of the patient's death.

**Ethnic background:** A patient's ethnic background needs to be identified to help in ensuring equal opportunity policy to the health services. It is also important to identify the patient's ethnic background to enhance hospital staff's awareness of a patient's culture and tradition, i.e. respect the patient's personal values and norms (interviewees' statements). This may be needed in the healthcare process.

**Occupation:** A patient's occupation is added to the record in case of the need to contact the patient's employer for information or in order to provide the employer with certain information, such as the patient's suitability for work or for granting a patient a break from work to aid the recovery process, as stated by one of the interviewees.

**Nationality:** A patient's nationality needs to be identified for three main reasons. The first reason it is needed is to establish the eligibility of the health services. This is due to the high number of visitors and non-nationals in SA. The second reason is to contact the patient's country in case of emergency. The third reason is that the patient's nationality can be used as an identity element.

**Date of Death:** Date of death needs to be part of the patient electronic record based on the interview analysis. This is needed for several reasons such as for legal, hospital management and national records.

**Table 5-2 : EPR, patient personal record**

| | Object |
|---|---|
| Patient Personal Record | Patient Hospital Record |
| | Patient NHS Number |
| | Patient Title |
| | Patient Surname |
| | Patient First Name |
| | Patient Photograph |
| | Patient Mother (Maiden) Name |
| | Date of birth |
| | Patient Telephone Number |
| | Gender |
| | Marital Status |
| | Home Address |
| | Religion |
| | Ethnic background |
| | Occupation |
| | Nationality |
| | Date of Death |

### 5.1.4 Patient Personal Related Record

Patient related record was identified as a group of information related to a patient that needs to be grouped as on identity. The information was identified from the literature review and the interviews. There are several related patient personal record items which need to be added to the patient electronic record due to their importance. This section presents these items and the justification for their inclusion in the EPR. Table 5.3 shows the main elements of EPR, patient personal related information and the following section presents the justification for including the items.

**Full Name of Next of Kin:** Patient family linkage was explored as an important item that needs to be included in the EPR. The full name of the next of kin needs to be included in the EPR for several reasons. These reasons include (i) in order to contact the kin in an emergency, (ii) consultation in the health care process, and (iii) helps in providing extra information regarding the patient.

**Next of Kin Telephone No:** This is needed in an emergency situation such as a deterioration in the patient's health or in case of the need for specific information or contact in case of patient death.

**Next of Kin Address:** Next of kin address is needed for correspondence with the kin in case further information is required and in an emergency.

**GP's Name:** The communication between the hospital and the patient is critical in the patient health care process (Sridhar et al., 2009; Becker, 2005). Therefore, the first step in the patient care process is identifying the patient's GP name so as to help in exchanging medical information and in providing the GP with the final patient medical condition and medication for the GP to follow it up.

**Surgery Name:** The surgery, local health care centre name is needed for correspondence with and identification of the surgery dealing with the patient, according to the interview analysis.

**Surgery Address:** The surgery address is needed for correspondence regarding the patient. This may include sending the patient's medical report or providing the hospital with any medical information required.

**Surgery Tel No:** The surgery telephone number needs to be included for the communication process between the patient and the surgery. This is needed for consultation in emergency cases and in the healthcare process. It is also needed to exchange medical information and in in clearing up issues in case of confusion, such as checking the patient's details or allergies.

**Workplace Name, Address and Telephone Number:** A patient's workplace name, address and telephone number are needed for correspondence regarding the patient's medical condition. Based on the interview analysis, this is needed to confirm whether the patient is fit to work or not. The workplace, i.e. nature of the patient's daily work, can help in the patient healthcare process. The workplace environment may have an impact on the patient's health.

**Donor Status:** Patient donation was explored in the literature and in the interviews as an important information source that needs to be available to the medical staff and to the hospital information system. Patient donation of body parts after death has become important information for the hospital and other national hospitals. This is mainly for the possibility of using such parts on other patients.

**Table 5-3 : EPR, patient personal related record**

| | Object |
|---|---|
| Patient Personal Related Record | First Kin Full Name |
| | First Kin Tel No |
| | First Kin Address |
| | GP Name |
| | Surgery Name |
| | Surgery Address |
| | Surgery Tel No |
| | Workplace Name |
| | Workplace Address |
| | Workplace Tel No |
| | Donor Status |

### 5.1.5 Patient Appointment Record

Table 5.4 shows patient appointment records main items and the following section presents the justification for including each item.

**Hospital Department Code:** The hospital information management system divides the hospital into departments based on medical specialization. The interviewees suggested on several occasions the importance and the need for the patient medical record to have a code to help to manage the information, trace the patient record and aid the access control process.

**Hospital Department Patient No (Code):** The interviews indicated that the hospital departments need to establish a patient code to help facilitate departments' activities and operations. This includes using the code for patient identification and facilitating communication among the department staff and other hospital departments. This can be created based on the EPR system and the medical staff at the department.

**Hospital Department Name:** The hospital department name is added to the patient medical record in order to be used as identification for the department's speciality and in the communication process, based on the interview analysis.

**Appointment Date and Time:** Patient appointment date and time is included in the EPR to help in (i) the hospital management time (i.e. to ensure effective use of the

hospital's human and physical resources) (ii) to help in tracing the patient's medical history.

**Discharge Date and Time:** The interviewees, in several statements, stated that the patient's appointment date and time needs to be included in the EPR to help in (i) the hospital management time (i.e. to ensure effective use of the hospital human and physical resources) (ii) to help in tracing the patient's medical history.

**Cancellation Date and Time:** Patient cancellation date and time needs to be included in the EPR to help in (i) the hospital management time (i.e. to ensure effective use of the hospital human and physical resources) based on the interview analysis.

**Hospital Department Consultant:** The interviewees, on several occasions, indicated the importance of the consultant's name being added to the EPR. This is mainly due to the medical profession structure within the hospital, identifying the medical team and usually the final decision on the patient medical case belongs to the consultant.

**Hospital Department Senior Nurse:** Hospital nurses play an important role in the patient health care process. The interviewees stressed the importance of and need to add the senior nurse to the EPR in order to identify the patient health care responsibility of the nurse.

**Referred from, and referred to:** The hospital department can be seen as a station in the patient's medical process. The patient is usually referred from one of the hospital departments such as the Emergency department or referred from his or her GP. This is needed to be included in the EPR to help trace the patient record in case more information is required (Sridhar et al., 2009; Becker, 2005).

**Comments:** The interview analysis found that EPR needs to have a space for comments. This is needed to add extra information which may be not included in the EPR. This gives the hospital and information management system the opportunity to add any information as needed. This item needs to be protected through access control.

**Updated By and Date (Staff Name):** The name of the staff member who updated the record and the date on which the update was carried out need to be added to the EPR

based on the interview analysis. This is needed to help in the justification for updating the record in the event of problems and for clarifying the process.

**Table 5-4: EPR, patient appointment record**

| | Object |
|---|---|
| Patient Appointment Record | Hospital Department Code |
| | Hospital Department Patient No (Code) |
| | Hospital Department Name |
| | Appointment Date and Time |
| | Discharge Date and Time |
| | Cancellation Date and Time |
| | Hospital Department Consultant |
| | Hospital Department Senior Nurse |
| | Referred from, and referred to |
| | Comments |
| | Updated By and Date (Staff Name) |

### 5.1.6 Patient Admission Record

Table 5.5 shows the patient admission record and the following section presents the justification for including each item. The following elements are based on the interview analysis and finding.

**Patient Admission Code:** The hospital information system is added to establish the patient admission record. This is needed to manage the patient admission process. The code can also help to track the patient.

**Arrival Date and Time:** A patient's arrival date and time needs to be added to the EPR as part of the patient medical care process.

**Arrival Method:** There are several possibilities for a patient's arrival. This may include in person, by ambulance, by private car or by taxi. This needs to be identified in the patient admission process. This is needed in case there is a need to trace the patient's history prior to the admission.

**Department (Ward):** EPR needs to include the department ward into which the patient is admitted. This depends on the patient's medical case because each department and ward deals with a specific illness and case and this helps to facilitate communication

and information exchange and sharing. This is included as an important part of EPR because of its role in facilitating hospital operation and management and locating the patient.

**Department Consultant:** The patient medical process needs to be under supervision of a senior specialist medical staff consultant. The consultant's name needs to be added to the EPR to help the medical process, by identifying the consultant and his team's responsibility to the patient's welfare in the hospital department.

**Diagnosis:** The EPR needs to include the patient's case, i.e. a diagnosis of the patient's case. This is needed as an important part of the medical care process. The diagnosis is the first step in the patient medical process. Diagnosis can also help to identify the consultant, team and department that need to take responsibility for the patient's care.

**Treatment Procedure:** The patient's treatment procedure needs to be added to the EPR for two main reasons. The first reason is that it is needed in the medical care process. The second reason is that it is needed in identifying the patient's medical history.

**Method of Discharging, Discharge Date and Time and Discharging Destination:** Patient discharging, discharging date and time were explored in the interviews as important items in the EPR. There is a need to include such information in order to help track the patient, help monitor the patient's health care and for hospital management.

**Table 5-5 : EPR, patient admission record**

| | Object |
|---|---|
| **Patient Admission Record** | Patient Admission Code |
| | Arrival Date and Time |
| | Arrival Method |
| | Transferred from and Transferred to |
| | Department (Ward) |
| | Department Consultant |
| | Diagnosis |
| | Treatment Procedure |
| | Method of Discharging |
| | Comments |
| | Updated By and Date (Staff Name) |
| | Discharge Date |
| | Discharge Time |
| | Discharging Destination |
| | Comments |

### 5.1.7 Non-medical information

Table 5.6 shows the patient non- medical information record and the following section presents the justification for including each item. The following elements are based on the interview analysis and findings:

**Hospital Name:** Hospital name is needed in the EPR to identify the hospital in the NHS system. The hospital name can also be used in the patient information seeking process.

**Hospital Address:** The hospital location needs to be included in the EPR in order to identify the hospital location, identify the hospital in case there are several hospitals with the same name, in the patient information seeking process, and to help the patient and relatives to locate the hospital.

**Hospital Telephone Number:** The hospital contact telephone number needs to be included in the EPR due to its importance in the communication processes. A communication process is needed for emergency contacts and in information exchange between patients and stakeholders.

**Ward Number:** The ward number is needed from hospital management structure. The ward number is an indication of the patient's location in his or her healthcare process. The ward number can also be used in the search process,

**Room Number:** The hospital ward may be divided into rooms. This is common in private hospitals. Therefore, it is important to include the room number in the electronic patient record. This is needed to facilitate the ward management process and to identify the patient's location.

**Bed Number:** A hospital ward has several beds and each bed is occupied by an individual patient. Each bed in the hospital needs to have a number. The number helps to facilitate managing the ward such as preparing the bed prior to the patient's arrival to the ward. The bed number can be critical to facilitate ward healthcare activity processes. Finally, the bed number can be used in communication among the ward medical staff.

**Nurse in Charge:** The EPR needs to include the nurse in charge of the patient health care process. This is needed to identify nurse responsibility, tracking the nurse in charge in case of investigation, incidents or complaint.

**Senior Nurse in Charge:** The senior nurse's main responsibility is to manage and take care of the patient during his or her stay in the hospital. Several interviewees stressed the importance of and the need to include the full name and employee number of the senior nurse in charge of the patient. They stressed that this is needed as part of the ward management structure and working process. It is also needed for tracking the senior nurse in charge of the patient during the patient's stay in the ward.

**Physician in Charge:** The patient medical process in the ward is the responsibility of the ward physician. The physician takes the responsibility for patients' medical care. This includes closely monitoring patients' health progress and stability. The interviewees stressed that the physician's name and employee number is needed for hospital and ward management needs and for tracking patients' medical history.

**Consultant in Charge:** The name of the consultant in charge of the hospital and the employee number or code need to be included in the electronic patient record. The interviewees and the literature indicated the importance of including the patient

consultant in charge of the patient in EPR. The main reasons for this inclusion are the importance and role of the consultant in decision making regarding the patient's healthcare. This includes diagnosis, treatment, medication and discharging the patient. The name of the consultant in charge is also needed in order to track the patient's medical history and responsibility.

**Table 5-6 : EPR, non-medical information**

| | Object |
|---|---|
| Non- medical information | Hospital Name |
| | Hospital Address |
| | Hospital Telephone Number. |
| | Ward Number |
| | Room Number |
| | Bed Number |
| | Nurse in Charge |
| | Senior Nurse in Charge |
| | Physician in Charge |
| | Consultant in Charge |

### 5.1.8 Patient Medical History

Table 5.7 shows the patient medical information history information record and the following section presents the justification for including each item. The following elements are based on the interview analysis and findings.

**Patient allergies:** Patient allergies are identified prior to the patient medical treatment and diagnosis as part of the health care process. This is needed part of the patient medical record information. Such information needs to be checked in any medical related decision making.

**Previous diagnosed illnesses:** Interviewees stressed the importance of including the patient's previous illnesses in the patient medical record both in traditional format and

in EPR. They expressed the view that recording a patient's previous illnesses helps in diagnosing the current patient medical record and in identifying appropriate medication.

**Blood Test:** Blood test results are included in the EPR due to their importance in diagnosing and in the patient recovery process. The interviewees stressed that the EPR needs to include details of all previous blood tests.

**Blood Pressure Test:** Patient blood pressure testing and recording is part of the patient medical record (Sridhar et al., 2009). Patient blood pressure needs to be recorded as part of monitoring patient medical condition and stability. This helps the medical staff to make decisions regarding the patient medical care process such as medication.

**Urine tests:** In interviews the urine test was considered to be one of the important tests in the patient healthcare process. The interviewees stressed that the urine test needs to be included in the patient's EPR. The main reason for this is that the urine test in EPR can be used in monitoring patients' medical health progress.

**Clinical test:** A patient in the hospital health care process goes through several clinical tests based on the patient's medical case. These tests need to be recorded as part of the diagnosis and treatment process. The interviewees' stressed repeatedly the importance of and the need for including such information. They stressed that recording the tests in EPR facilitates quick access to and checking of such information.

**X-ray:** X-ray records of the patient were identified as one of the records needing to be included in the EPR due to their importance on the patient diagnosis and medication process. This may include digital capture and storage of X-ray, (The Health Committee, 2007) (Sridhar et al., 2009). Its inclusion helps easy access to present and past x-rays and easy navigation through the x-ray.

**Surgical Operations:** Patient previous surgery details need to be included in the EPR based on the interviewees' opinions. This includes date, time, purpose, and process used in the surgical operations. This historical information need to be available to the medical staff.

**Family medical history:** Family medical history such as the father's and mother's medical history is one of the processes used to help in understanding and diagnosing

patient condition, based on the interviewees' comments (medical doctor). It was stressed that the generic relationship between the patient and his/her family needs to be considered in the diagnosing process. This information needs to be available in the EPR to help access such information any time the patient visits the hospital.

### 5.1.9 Patient Medication

Table 5.8 shows the patient medication record and the following section presents the justification for including each item. The following elements were based on the interview analysis and findings.

**Medicine 1:** Patient usually given one or more medicine as medication for the patient recovery. The name of such medicines need to be recorded and must be available for the next patient visit. This is needed as part of identifying the influence and role of the medicine in the recovery process.

| | Object |
|---|---|
| **Patient Medical History** | Patient allergies |
| | Previous diagnose illness |
| | Blood test |
| | Blood Pressure Test |
| | Urine tests |
| | Clinical test |
| | X-ray |
| | Surgical Operations |
| | Family medical history |

Table 5.7: Patient's medical history

**Medicine Date:** Based on the interviewees, date of giving particular medicine needs to be recorded. This represents the historical medical information. Such information needs to be available to the medicine staff to help in recovery process and in medication

**Medicine Dose:** Medicine dose is an important element of the subscribed medicine. The effect of the medicine depends on the dose subscribed by the senior medical staff. Such information needs to be provides and available on the EPR to help in subscribing the new medicine.

**Injection 1:** Subscribed injection name needs to be included in the EPR based on the interviewees' opinion. They stressed the need of such information in the patient recovery process. This information in EPR helps the medical staff accessing such information at reasonable time and effort.

**Injection Date:** Date of injection is an important element of injection record. Injection date included to record and makes it available to the medical staff. This helps subscribing the next injection and in the patient health progress.

**Injection Dose:** Subscribed injection dose needs to be recorded in EPR due to its important in the patient medication. The injection dose information needs to be available to the medical staff to help in medication decision making process.

## 5.2 ISM Security Policy Model

National Health Services information security systems policy has become an important part of the NHS strategy to meet the needs to comply with

**Table 5-8 : Patient medication**

| | Object |
|---|---|
| **Patient Medication** | Medicine 1 |
| | Medicine Date |
| | Medicine Dose |
| | Injection 1 |
| | Injection Date |
| | Injection Dose |

NHS stakeholders' requirements and the national and

international regulatory. This requires NHS authority to take a serious considerations and a well-established planning to achieve effective NHS information security policy. ISM information security modelling is an essential part of the information security policy steps development in the National Health Services. It provides frameworks and theoretical background for developing and implementing effective information security policy. This section presents initial models for developing effective information security for NHS in SA. It is expected the proposed models will be evolved and developed further based on the outcomes of the models evaluation. The proposed models development is based on the literature survey and fieldwork data analysis.

The first part of this section presents and discusses a framework for investigating the current situation of the information security policies in SA NHS. This research based on the literature survey and interviewees opinions proposed four initial models for NHS information security models, see Figure 5.2. These models are NHS Information Security Framework Model, Information security system process model, access control model, information security system behaviour model.

These models aim to establish a framework for the information security policy in the SA NHS. This is needed to organize and manage the security system activities within the NHS efficiently and effectively.

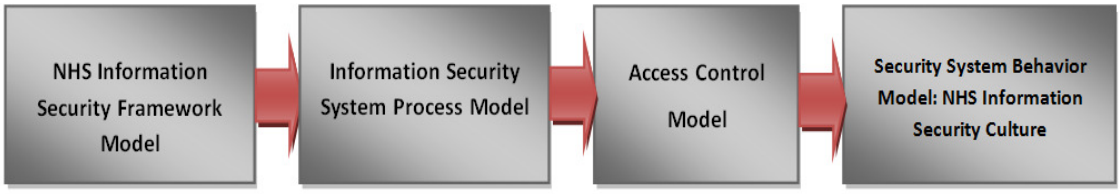



**Figure 5.2 : Information Security Systems policy framework**

### 5.2.1 NHS Information Security Systems: Current Situation

One of the main objectives of this research is to investigate the current situation of the information security system in Saudi Arabia NHS. The proposed framework model for this investigation is shown in Figure 5.3. The proposed framework model is based on investigating and exploring seven information security policy issues explored and identified in the literature survey and the fieldwork data analysis. The first issue that needs to be investigated and explored in the NHS current situation is the technical issue.

#### *5.2.1.1 Current Technical Situation*

This issue aims to investigate the current information security systems, capability and functionality of the system, used and the current technical problems facing establishing effective information security policy. The technical situation also needs to take in consideration the staff technical skills and competence.

The current technical situation indicated that the hospital trained selected staff in USA based on the contract between the hospital and the system provider. The interviews indicated each of the trainee asked to train other member staff in the system. The problems raised is that any technical changes in the system, modifying the system, or re-designing certain parts of the system is not available due to the fact the system designed and developed in USA. It is also there is a large number of the staff lack confidence in using the system due to lack the technical skills and competence. Therefore, the hospital authority needs to take in consideration the technical issue in the information security process.

#### *5.2.1.2 Organisation security system culture*

The second issue is to investigate the current NHS as an organisation security system culture. This includes the current practice norms among the NHS stakeholders in compliance with the current information security policies. The current hospital culture requires promoting information security, especially patient record. Patient record accessed and released with a checking and taking in consideration the privacy of the patient personal information. The information security process needs to take in consideration the hospitals culture to protect EPR.

#### *5.2.1.3 National regulatory bodies' compliance*

The third issue that health services is the current national regulatory compliance. NHS represents an important and one of the major national services sectors in SA. There is a lack of national policies that NHS organizations need to comply with regarding health information. Therefore, this issue aims to investigate the current national policies and requirement regarding the information security systems that NHS needs to comply with.

The Ministry of Health and Central government have brief and adequate generic policy regarding health services information security.

#### *5.2.1.4 International regulatory bodies*

Saudi NHS also needs to comply with international regulatory bodies, issue four. This issue aims to explore the international regulatory policies and requirements that NHS needs to comply with. One of these bodies is the International Human Right. The human right requires organisations to treat individual with respect and as unique identity without any prejudice against the individual colour, religion, sex and nationality.

#### *5.2.1.5 Current information security policy used*

Security policy process is a dynamic process. NHS authority needs a continuous improvement process of its security policy. This is mainly due to sharp changes in technology that used in health services information and expand in health services information. The current information security has been written relatively long time ago with little emphasis on the electronic patient record access. There is a need to consider the current security policy used and identify its weaknesses and strength and particularly the patient right and the use of electronic patient record.

#### *5.2.1.6 Security formulating process*

The current security formulating process is limited to few people mainly from the ISM personnel and management. The security formulating process needs to take in consideration of several factors. These factors include feedback from the security policy users to identify their weaknesses and strengths. This may be in the form of feedback forms or one-to-one interviews with the main stakeholders of the information security. The interviews indicated the need and expand number of people involved in formulating and reviewing the information security policy. It also indicated the need for involvement different discipline in the process. This includes the medical profession rather than restricted on the ICT personnel and management personnel.

The outcomes of the current situation analysis help in understanding and knowledge of the situation. The understanding and the outcomes of the current situation will also be used and referred to in the discussion the outcomes of this research.

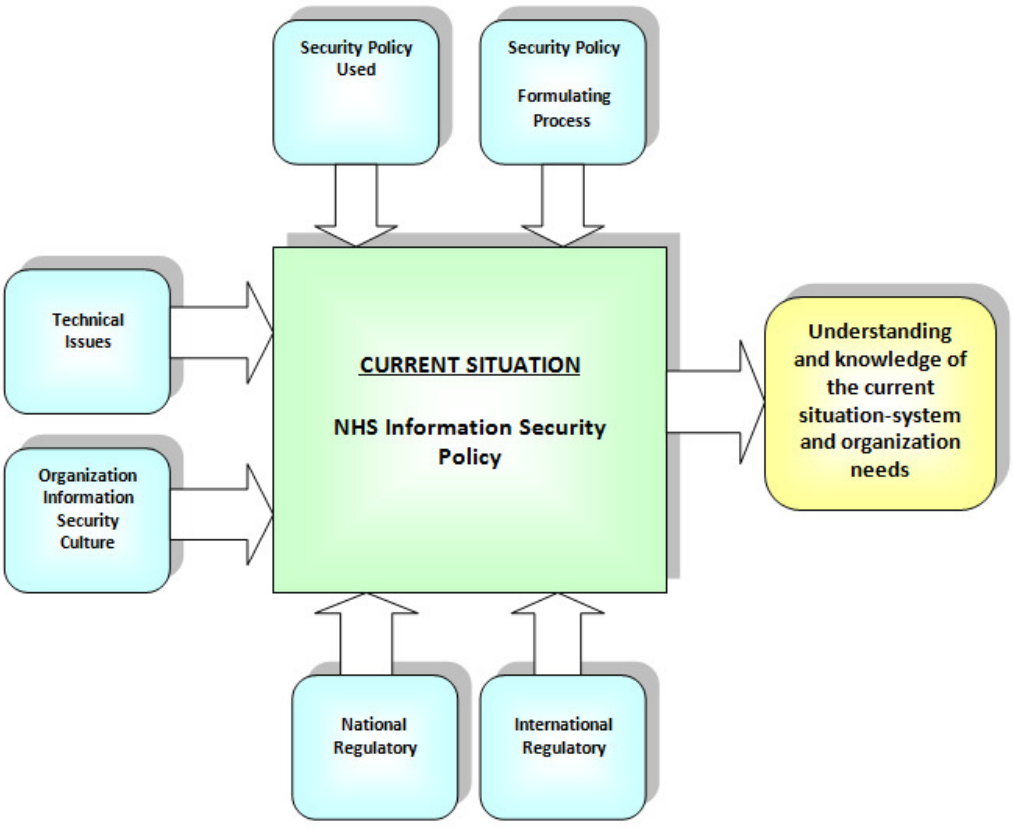



**Figure 5.3 : Proposed framework for investigating current situation of Information Security systems policy**

### 5.2.2 NHS Security System Framework Model

The National Health Services (NHS) is one of the major public service providers in SA. They are a large organization handling a large number of sensitive electronic records and information on a daily basis. Security of information has become a requirement due to several pressures from several health service stakeholders such as patients and regulatory bodies. The National Health Services need to establish a framework model for the security systems to help cope with the need for an efficient and effective security system.

**Main Drives for NHS Security Systems:** The framework starts with identifying the main drives for NHS security systems. The NHS authority needs a justification for any strategic plan and actions due to the sensitivity of their activities and the cost. These drives need to be analysed critically to provide a strong case for financial and human resources commitment by the SA NHS. Therefore, identifying the main drives for the NHS security system is a critical part of the framework model as this may change due to

changes in the internal NHS or external business environment, such as changes in legislation and technology. Once the main drives are identified, the NHS then needs to identify an information security mission statement.

**Mission Statement:** The mission statement needs to reflect the values of the NHS records, information confidentiality and security. The SA NHS needs to reflect authority vision and strategic plan for security and confidentiality of the NHS record. The mission aims to motivate NHS employees and stakeholders to ensure information security and security awareness during handling and transmission of medical information such as electronic patient records. Based on the main drives and the mission statement, NHS needs to establish the information security system objectives.

**Objectives:** The NHS vision and strategy need to be executed through several objectives. These objectives should be focused on information security. The objectives need to be established and identified by SA NHS senior management. Once the objectives are identified, the NHS needs to establish information security system models.

**SA NHS Security System:** This study argued that the NHS needs to establish three main security policy models. These information security policy models include:

**Electronic Patient Record Security Policy:** Electronic patient record is the core element of the SA NHS records. There are several drives for the NHS to establish an efficient and effective EPR security policy.

**NHS Staff Electronic Record Security Policy:** SA NHS staff records and information are private and sensitive information. The SA NHS is obliged to ensure the security of handling and transmission of such information. The SA NHS information security system needs to establish a specific policy for staff information security.

**NHS Management Security Policy:** The other policy is the management policy. This policy aims to control the management access procedures and power of changing security processes and procedures.

**NHS Security System: Information Security Implementations:** Once the information security policy is identified, an implementation policy needs to be

established. This policy aims to establish processes and procedures to ensure effective implementation of the security policies.

**NHS Security System; Evaluation Policy:** Finally, the framework model closes with an evaluation policy. The evaluation policy needs to establish the processes, procedures and policies for evaluating the information security systems. The evaluation policy aims to improve the quality of the security systems by identifying the strengths and weaknesses of the systems and the following action policies.

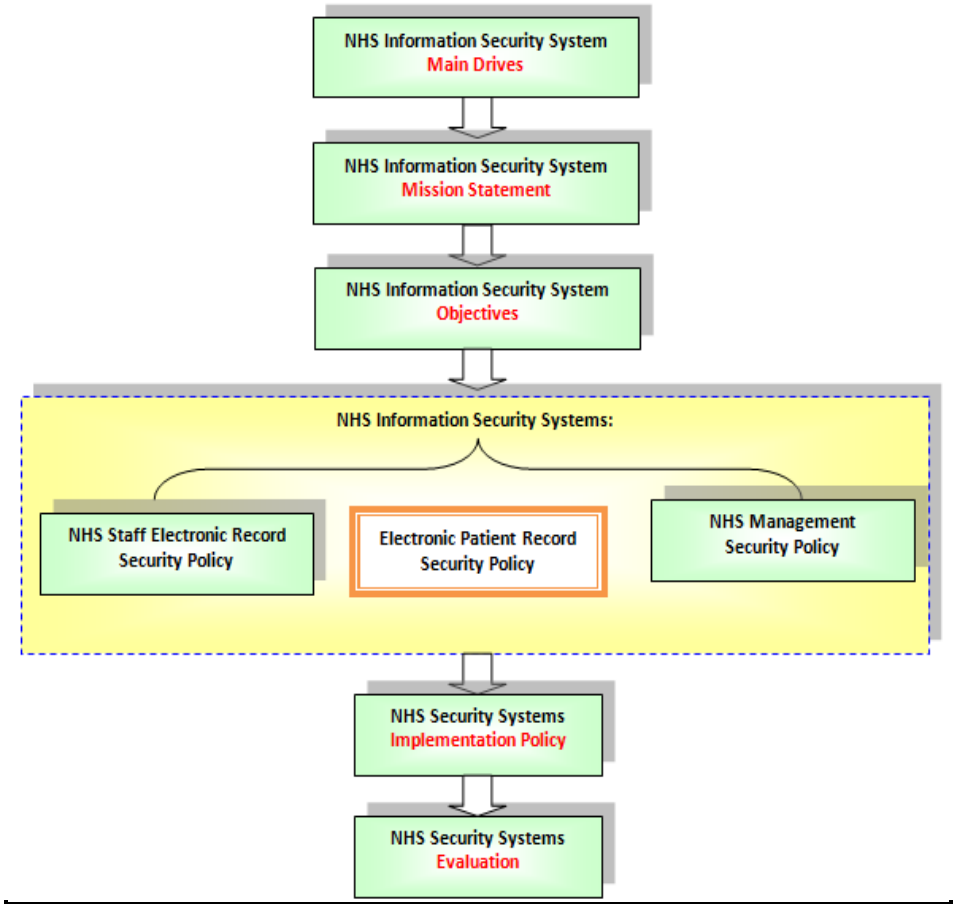



**Figure 5.4 : SA NHS Information Security framework model**

### 5.2.3 Information Security System: Access Control Model

The information security system aims to establish access control strategy based on two main factors. The first factor is user needs. The needs are based on the job role and responsibilities of the user. The second factor is the type of information, or information sets. The model helps the SA authority to establish information security policy based on this model. The model consists of the following main elements:

*5.2.3.1 ISM Group Users*

Figure 4.5 shows an initial model for NHS information security. The model divides the NHS ISM system to two main groups of users at four access control levels. The first level is the NHS staff and the second level is the external stakeholder users such as police, social workers and NHS inspectors (regulatory bodies).

**NHS Staff:** The NHS services are the second largest national services in the Kingdom. There is a large number of staff and patients. The large number of ISM users needs to be controlled through an effective and efficient information security policy. The NHS staff information users can be classified into the following groups

- Clinical Staff
- Senior-clinical Staff
- Administrators
- Senior-administrators
- ISM/ICT Technical Staff

**NHS Stakeholders:** There are several NHS stakeholders in SA. The stakeholders interact with the NHS for various reasons. The stakeholders may need to access certain NHS information and data, some of which may be patient records. The main stakeholders include:

- Police
- Social workers
- NHS Suppliers
- NHS Inspectors (Regulatory)
- Public

*5.2.3.2 ISM Data and Information*

NHS has a large quantity of data and information. It is also important to stress that the volume of data and information is increasing due to an increase in the number of health services hospitals and specialised hospitals. Awareness of health information by the SA health authority and medical staff has helped to protect the data and information. NHS data and information are classified to three levels of data and information depending on the sensitivity of the data and information.

The proposed model has several levels of access control to the NHS data and information, based on the developed electronic patient record. Therefore, this needs to assign certain roles to manage and control the access. The access will be controlled based on the type of information group that the user needs according to their role and responsibilities. The roles will be based on the roles, users and privileges, role hierarchies; each user will have certain access to a certain level of information access.

The first level is control access 1 (see Figure 5.5): This level contains generic health information such as advice to the public regarding the most common diseases and health issues. The access should be opened to the public with restrictions on any editing and deleting the database information. A set of policy roles needs to be established to manage access control level.

The second level, access control level 2, is designed to give access to the non-clinical staff such as the NHS administration staff. This level gives access to the administration database, such as entry of patients' identity information. This helps to identify the patients. This is needed to ensure that care is provided to the intended patients and can also be used in communication with NHS stakeholders and for locating the patient.

The third level of information is the patient's personal information, such as home telephone number and mobile number for example.

#### *5.2.3.3 Patient Personal Related Record*

This level is for information-related information. This includes, for example, the patient's records.

The third level is the access control level 3. This level is provided only for medical staff, such as the physicians and the nurses. This level controls access to certain medical information regarding patients. This access is also controlled by a certain user's roles.

The fourth level is the access control level 4. This level is provided only to certain senior medical staff access. This level contains sensitive and personal medical situation. The senior medical staff has access to editing and updating the database. This access is controlled by certain roles.

The patient record is critical and is an important record in the health services, since in health services organizations there are several medical related staff having certain roles in the patient health service. The subject role in the patient health care process is the key element in the subject access to the patient electronic record. Due to the privacy nature of the patient reagrding medical and patient rights, the access should be restricted to anyone who is not contributing to or has a role related to the accessed patient record. Therefore, there is a need to design the patient electronic record access system based on this information need. Anderson (1996) stated:

> "*Each identifiable clinical record shall be marked with an access control list naming the people or groups of people who may read it and append data to it. The system shall prevent anyone not on the access control list from accessing the record in any way*" (Anderson, 1996).

Access control mechanism design in an information system is needed to ensure to limit any actions or operation that a legitimate user can perform (Sandhu, 1996). This is based on the individual user's role in the patient health welfare. The first step in the patient electronic medical record is the owner of the patient electronic record. There is an argument for the main owner of the record. In the UK, there is a debate regarding the legitimate medical record owner (Hodge, 2003; Ross, 2003; Anderson, 1996). However, Iacovino (2004) argued that the owners of the records are the patient, medical authority and the medical practitioner. Alhaqbani (2008) argued that patients have the right to their own medical record.

It is expected that the matrix will be evolved and modified after the fieldwork visit. The visit will discuss the proposed matrix and use the outcomes of the discussions in developing the final patient medical record matrix. The matrix is based on dividing the access based on groups of discipline. The discipline is based on the role of the group users. However, this may need to be divided further into subgroups depending on the organization structure and the nature of the patient case. For example, the physician group can be divided into subgroups depending on specialization. The nurses' group can also be divided into subgroups depending on their role within the hospital.

- **Administrator:** Based on the interviews and the literature (Becker, 2005), hospital administrators such as the hospital receptionist and ward receptionist are the first contact between the patient and patient stakeholders. They represent part of the patient medical health care management process. They need to access certain EPR elements to help manage the patient medical process effectively.

  The administrator's access right is based on the administrator's role in the patient health services process. Access should be based on the administrator role in the administration process within the group.
- **Nurse:** Hospital nurses play an important role in the patient medical care process during the patient hospital visiting and staying. They are one of the main users of the EPR (Ferreira et al., 2007; Williams et al., 2008; Ferreira et al., 2008). They provide daily care and look after patient welfare. Therefore, the nurses need certain information within the EPR to help carry out their job activities efficiently. The nurses' role needs to give them access to medical records that reflect their role in the patient health services process (Dekker et al., 2007).
- **Medical Doctor-Physician charge of the patient:** Medical doctor is one of the main EPR users (Ferreira et al., 2007; Lovis et al., 2007; Sridhar et al., 2009), (Ferreira et al., 2008). Hospital medical doctors are responsible for diagnosing, monitoring, and checking the patient's medical condition. One of the main jobs is to record patient medical progress on the EPR.

  A doctor may read the personal information section of the EPR (Sandhu, 1996) and also may read and update medical data (Dekker et al., 2007).
- **Anaesthetist:** Anaesthetist is identified as one of the group of EPR users (Williams et al., 2008). They need to be included in the EPR due to the nature of their jobs. They need to check several types of information on patients.
- **Hospital Medical Physician Consultant:** Hospital medical consultant is the senior subject in the patient health care and one of the main EPR users (Lovis et al., 2007). They are usually team leaders for a group of medical doctors and nurses and are the main decision makers on patient diagnosis and medication.

They need to access certain information in the EPR to help carry out their jobs efficiently and effectively.

They need to read and write on the patient medical record to ensure effective health care services to the patient and personal information (Hu et al., 2006).

- **Radiologist:** Radiologists were discussed in the interviews and in the literature (Williams et al., 2008) as an important group of users of the patient medical record.
- **Management Information System, MIS Members (ICT Administrator):** Looking at the essential IT security administration processes, access control and granting access rights to users are of central importance. Their rights are mainly technical and they have no right to change any of the patient medical records (Kuhlmann et al., 2003).
- **Patient:** The patient is one of the main EPR users (Ferreira et al., 2007; Ross, 2003; Ferreira et al., 2008). A patient may read and update the personal information section.
- **NHS Regulatory (Audit):** NHS is one of the sensitive public services. There is a need to check the performance of the NHS on a regular basis to ensure the quality of services and to identify the strengths and weaknesses of the services. This is needed as part of the continuous improvement process in the healthcare services. One of the approaches used to improve the healthcare services is the use of internal and external audit. The main aim of the audit is to identify the strengths and weaknesses in the health services towards providing a high quality of service to patients. Therefore, the audit group needs to access certain information regarding patients records, particularly statistical data.
- **Senior Manager:** Senior manager has the authority within the health services that determines access right of the information system users (Hu et al., 2006).
- **Pharmacists:** Pharmacists in health service organizations provide the appropriate medication based on the physician and consultant subscript. Therefore, the pharmacist need access to the patient medical records (Williams et al., 2008; Ferreira et al., 2008). They need the access to report on the patient's medication. The access should only reflect their role, i.e. read the patients' personal details and the medication details.

- **Medical Technician:** There are several medical technicians in the hospital as part of the medical support team. They play an important role in the patient medical care process. They need access to the EPR (Lovis et al., 2007; Williams et al., 2008) to help carry out their job efficiently and effectively.
- **Medical Student:** Medical students spend time in hospital as part of their studies as a requirement to acquire the appropriate experience and competence. They need to access EPR (Lovis et al., 2007; Williams et al., 2008).
- **Receptionist:** The health services receptionist is the first contact between the patients, the patients' relatives and patient stockholders. The receptionist is usually asked for certain information regarding the patient. The interview analysis indicated that there is a need to give the receptionist the access to create information to facilitate healthcare receptionists such as the patient name, ward number as an examples.

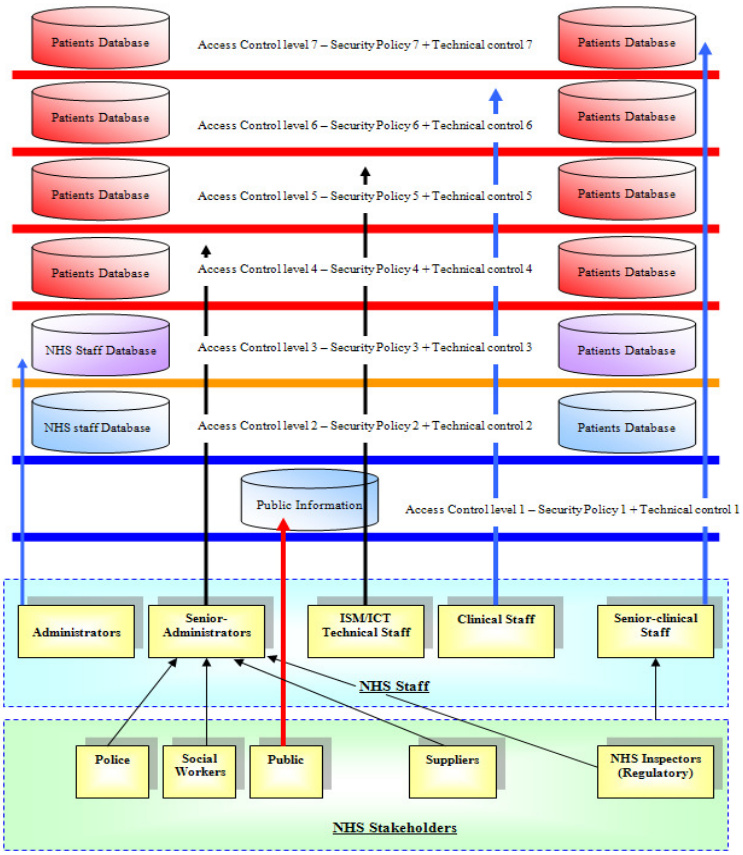



**Figure 5.5 : Access control model**

# CHAPTER SIX:

# EVALUATING ACCESS TO ELECTRONIC PATIENT RECORDS QUESTIONNAIRE ANALYSIS

Objectives

- Identify SA-NHS staff information access to be based on their role in the patient care process.
- Present the results of the questionnaire.

# 6 CHAPTER SIX: EVALUATING ACCESS TO ELECTRONIC PATIENT RECORDS QUESTIONNAIRE ANALYSIS

## 6.1 Introduction

This chapter presents the analysis of the evaluation questionnaire responses. SPSS software was used for this analysis. The evaluation's main purpose was to establish access control policy for accessing EPR, assessing the governmental reality compared to their policy. The users' access was based on having Read access to the EPR, Update access or no requirement for access. The Read access allows the user ONLY to access the information without any right to delete, update or edit the information. On the other hand the Update access gives the user the right to modify the EPR. It is also important to stress that all changes are recorded and logged by the system. The evaluation was based on distributing a questionnaire (see Chapter 3) asking respondents to express their experience of EPR security in the hospital.

## 6.2 Hospital Staff

The questionnaire was distributed to staff from different disciplines in order to help to identify their needs from the patient electronic record (Chapter 3). Table 6.1 shows the role of the respondents, and the frequency, and percentage of the subject sample.

| | Frequency | Percentage (%) |
|---|---|---|
| Consultant | 2 | 4.3 |
| Registrar | 3 | 6.5 |
| Resident | 4 | 8.7 |
| Anaesthetist | 3 | 6.5 |
| Medical Student | 3 | 6.5 |
| Nurse | 4 | 8.7 |
| Matron | 2 | 4.3 |
| Pharmacist | 3 | 6.5 |
| Medical Lab Technician | 2 | 4.3 |
| Radiologist | 2 | 4.3 |
| Research/Development Coordinator | 2 | 4.3 |
| Senior Manager | 2 | 4.3 |
| Head of Department | 2 | 4.3 |
| MIS Member | 3 | 6.5 |
| NHS Regulatory (Audit) | 1 | 2.2 |

| | | |
|---|---|---|
| Administrator | 4 | 8.7 |
| Receptionist | 4 | 8.7 |
| Total | 46 | 100.0 |

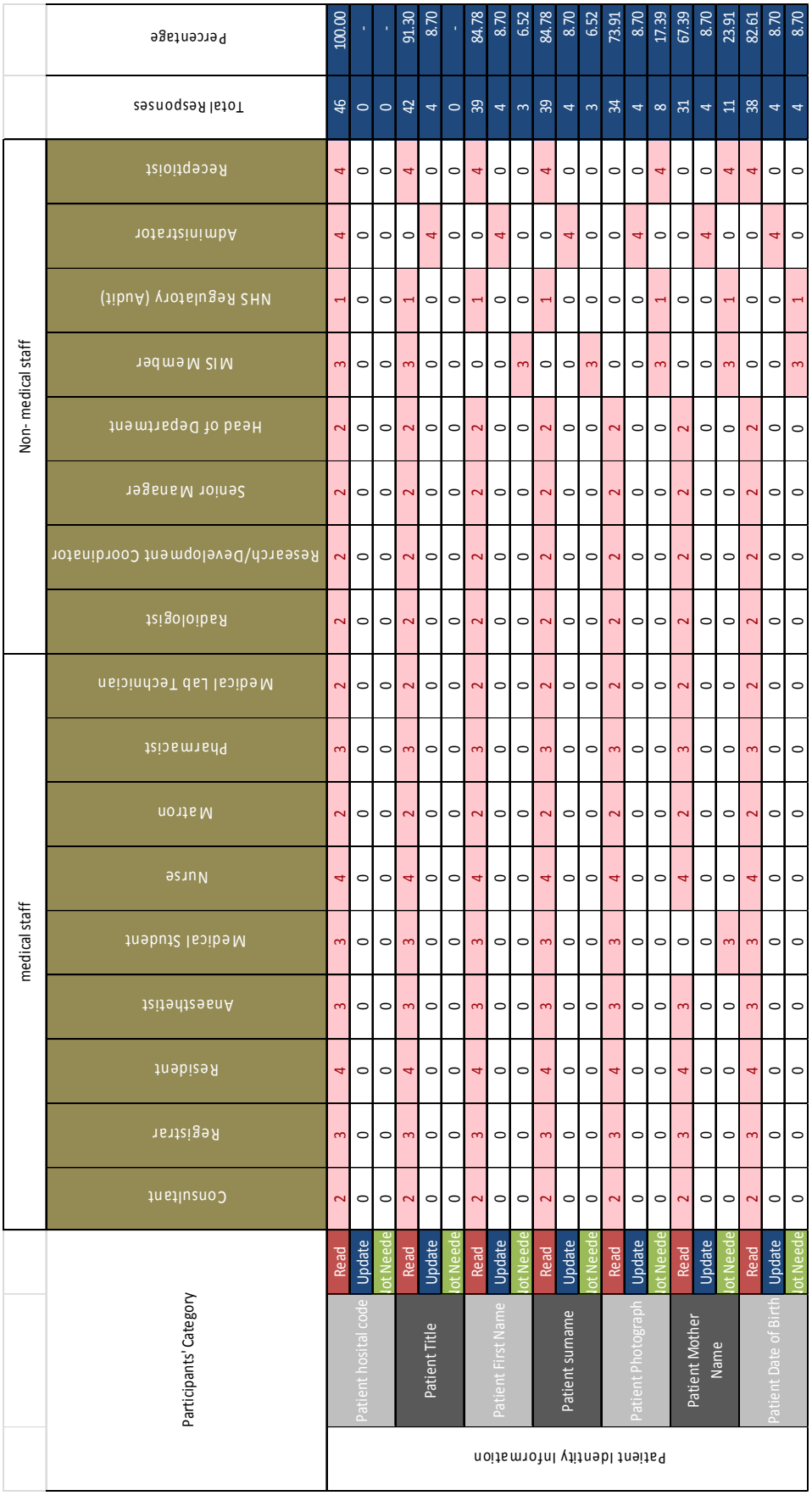
**Table 6-1 : Hospital sample selection based on role**

## Patient Identity Information

The first section of the analysis is focused on the patient's identity information. Table 6.2 shows the responses of medical and non-medical staff participants. The table indicates that all participants (medical and non-medical groups), 100% (46 out of 46), have Read access to the hospital code. This is mainly due to the fact that the hospital code was inserted during the installation process of the system. The hospital policy is based on inserting the hospital code to the EPR system as part of the management system. The information was inserted prior to the actual use of the EPR. This is due to the fact that this information is fixed for all the EPR users and has no security status among the hospital employees, whether medical or non-medical staff.

Medical staff members indicated that they have Read access only to the rest of the patient's identity information, namely patient's title, surname, first name, photograph, mother name and date of birth . The hospital administration strategy stressed that inserting patient identity information is part of the hospital administrator's job role and responsibility. The decision aims to reduce any waste of the medical and medical support staff's time and effort. The analysis indicated consistent responses. Medical lab technicians, radiologists, research/development coordinators and senior managers indicated that they have Read access only. Administrators have access to update the patient identity information. NHS regulatory subjects have Read access to hospital code, patient title, patient first name and patient first name. The NHS regulatory subjects have stated that they do not need to access patient photograph, patient mother name and patient date of birth. MIS members have read only access to the hospital code and the title of the patients.

The main aim of this section is to identify the EPR users need to access EPR. This is needed in the process of establishing information and access control policies.



| Participants' Category | | medical staff | | | | | | | | | | Non- medical staff | | | | | | | | | | Total Responses | Percentage |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Consultant | Registrar | Resident | Anaesthetist | Medical Student | Nurse | Matron | Pharmacist | Medical Lab Technician | Radiologist | Research/Development Coordinator | Senior Manager | Head of Department | MIS Member | NHS Regulatory (Audit) | Administrator | Receptiolst | | | | | |
| Patient Identity Information | Patient hosital code | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 1 | 4 | 4 | | | | 46 | 100.00 |
| | | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | 0 | - |
| | | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | 0 | - |
| | Patient Title | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 1 | 4 | 4 | | | | 42 | 91.30 |
| | | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | 4 | 8.70 |
| | | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | 0 | - |
| | Patient First Name | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 1 | 4 | 4 | | | | 39 | 84.78 |
| | | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | 4 | 8.70 |
| | | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | | | | 3 | 6.52 |
| | Patient surname | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 0 | 1 | 0 | 4 | | | | 39 | 84.78 |
| | | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 4 | 8.70 |
| | | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | | | | 3 | 6.52 |
| | Patient Photograph | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 0 | 1 | 0 | 4 | | | | 34 | 73.91 |
| | | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 4 | 8.70 |
| | | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 8 | 17.39 |
| | Patient Mother Name | Read | 2 | 3 | 4 | 3 | 0 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 0 | 0 | 0 | 4 | | | | 31 | 67.39 |
| | | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 4 | 8.70 |
| | | Not Needed | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 11 | 23.91 |
| | Patient Date of Birth | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 0 | 0 | 0 | 4 | | | | 38 | 82.61 |
| | | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 4 | 8.70 |
| | | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 1 | 0 | 0 | | | | 4 | 8.70 |

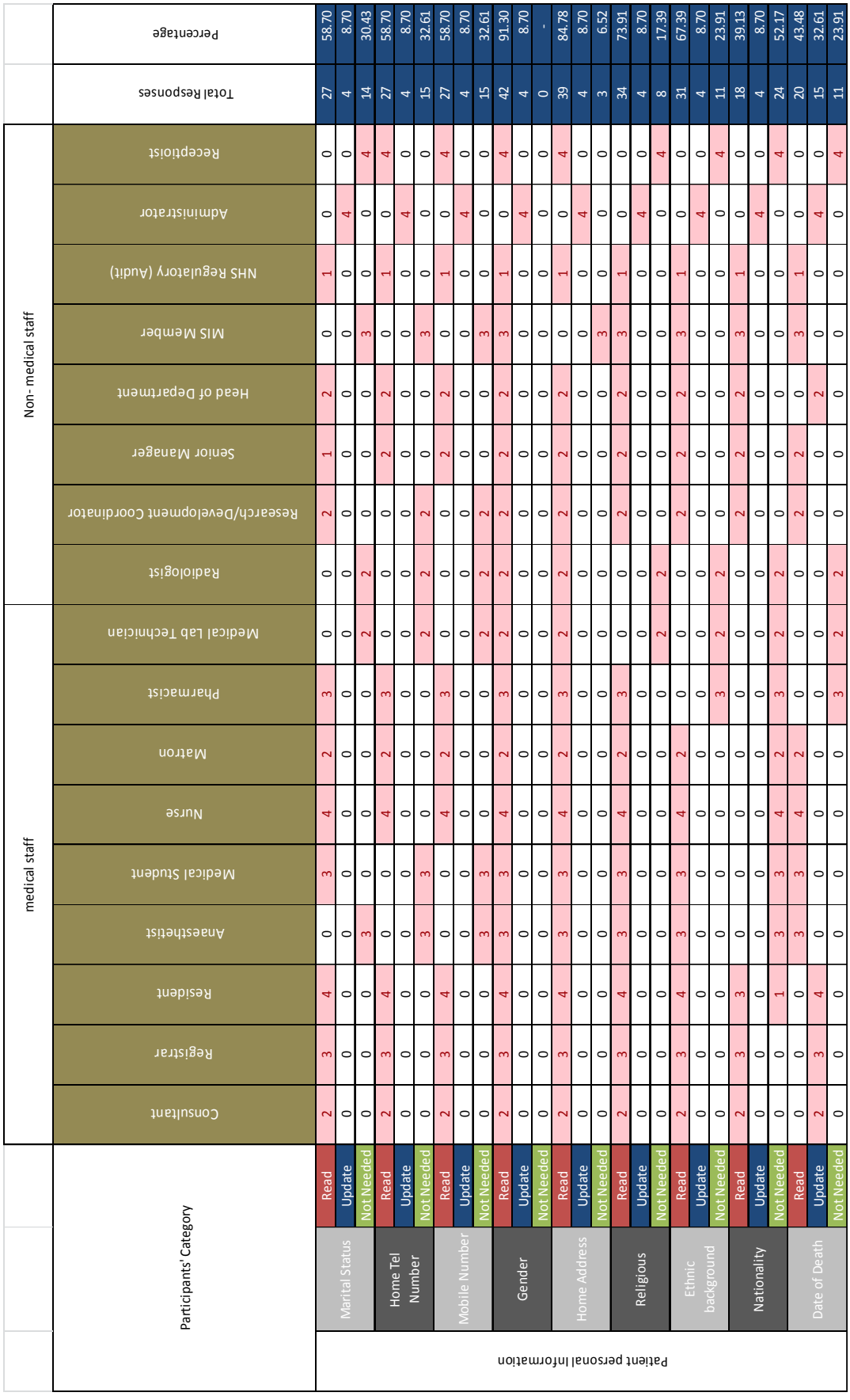
**Table 6-2 : Patient Identity Information**

## Patient Personal Information

Table 6.3 shows patients' personal information for medical and non-medical staff. Consultants, registrars and residents have Read access information and they have only Update access to the patient's date of death. Nurses and matrons have Read access to the information apart from patient's nationality: they indicated that they do not need such information. Anaesthetists indicated that they have Read access to patient's gender, home address, religion, ethnic background and date of death. They also indicated that they do not need to access a patient's marital status, home telephone number, mobile number or nationality. Medical students have Read access to marital status, gender, home address, religion, ethnic background and date of death.

For non-medical staff, staff have Read access to the patient's gender, and to the patient's home address apart from the NHS members. Administrators indicated that they have Update access for the patient's personal information. Receptionists indicated that they have read access to patient's home telephone number, mobile number, gender and home address. They also indicated that they do not need to access a patient's marital status, religion, ethnic background, nationality and date of birth. Medical lab technicians and radiologists indicated that they have Read access to patient's gender and home address only. Pharmacists have Read access to the patient's marital status, home telephone number, mobile number, gender, home address and religion. MIS members indicated that they have Read access to the patient's gender, religion, ethnic background and date of death.

The main aim of this section is to provide in-details patient information. This is needed in healthcare process, identifying the patient, establish information and access control policies.



| | Participants' Category | Consultant | Registrar | Resident | Anaesthetist | Medical Student | Nurse | Matron | Pharmacist | Medical Lab Technician | Radiologist | Research/Development Coordinator | Senior Manager | Head of Department | MIS Member | NHS Regulatory (Audit) | Administrator | Receptionist | Total Responses | Percentage |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Patient personal Information | Marital Status | 2 | 3 | 4 | 0 | 3 | 4 | 2 | 3 | 0 | 0 | 2 | 1 | 2 | 0 | 1 | 0 | 0 | 27 | 58.70 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 8.70 |
| | | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 3 | 0 | 0 | 4 | 14 | 30.43 |
| | Home Tel Number | 2 | 3 | 4 | 0 | 0 | 4 | 2 | 3 | 0 | 2 | 0 | 2 | 2 | 0 | 1 | 0 | 4 | 27 | 58.70 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 8.70 |
| | | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 3 | 0 | 0 | 0 | 15 | 32.61 |
| | Mobile Number | 2 | 3 | 4 | 0 | 0 | 4 | 2 | 3 | 0 | 2 | 2 | 2 | 2 | 0 | 1 | 0 | 4 | 27 | 58.70 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 8.70 |
| | | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 3 | 0 | 0 | 0 | 15 | 32.61 |
| | Gender | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 0 | 2 | 2 | 2 | 2 | 3 | 1 | 0 | 4 | 42 | 91.30 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 8.70 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - |
| | Home Address | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 0 | 1 | 0 | 4 | 39 | 84.78 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 8.70 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 6.52 |
| | Religious | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 3 | 1 | 0 | 4 | 34 | 73.91 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 8.70 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 3 | 0 | 0 | 4 | 8 | 17.39 |
| | Ethnic background | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 0 | 0 | 0 | 2 | 2 | 2 | 3 | 1 | 0 | 4 | 31 | 67.39 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 8.70 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 2 | 0 | 0 | 0 | 3 | 0 | 0 | 4 | 11 | 23.91 |
| | Nationality | 2 | 3 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 3 | 1 | 0 | 0 | 18 | 39.13 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 8.70 |
| | | 0 | 0 | 1 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 0 | 3 | 1 | 0 | 4 | 24 | 52.17 |
| | Date of Death | 0 | 0 | 0 | 3 | 3 | 4 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 3 | 1 | 4 | 0 | 20 | 43.48 |
| | | 2 | 3 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 15 | 32.61 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 11 | 23.91 |
| | | Read | Update | Not Needed | Read | Update | Not Needed | Read | Update | Not Needed | Read | Update | Not Needed | Read | Update | Not Needed | Read | Update | Not Needed | Read | Update | Not Needed | Read | Update | Not Needed | Read | Update | Not Needed | Read | Update | Not Needed | Read | Update | Not Needed | Read | Update | Not Needed | Read | Update | Not Needed | | |
| | | medical staff | | | | | | | | | | Non- medical staff | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Table 6-3 : Patient Personal Information**

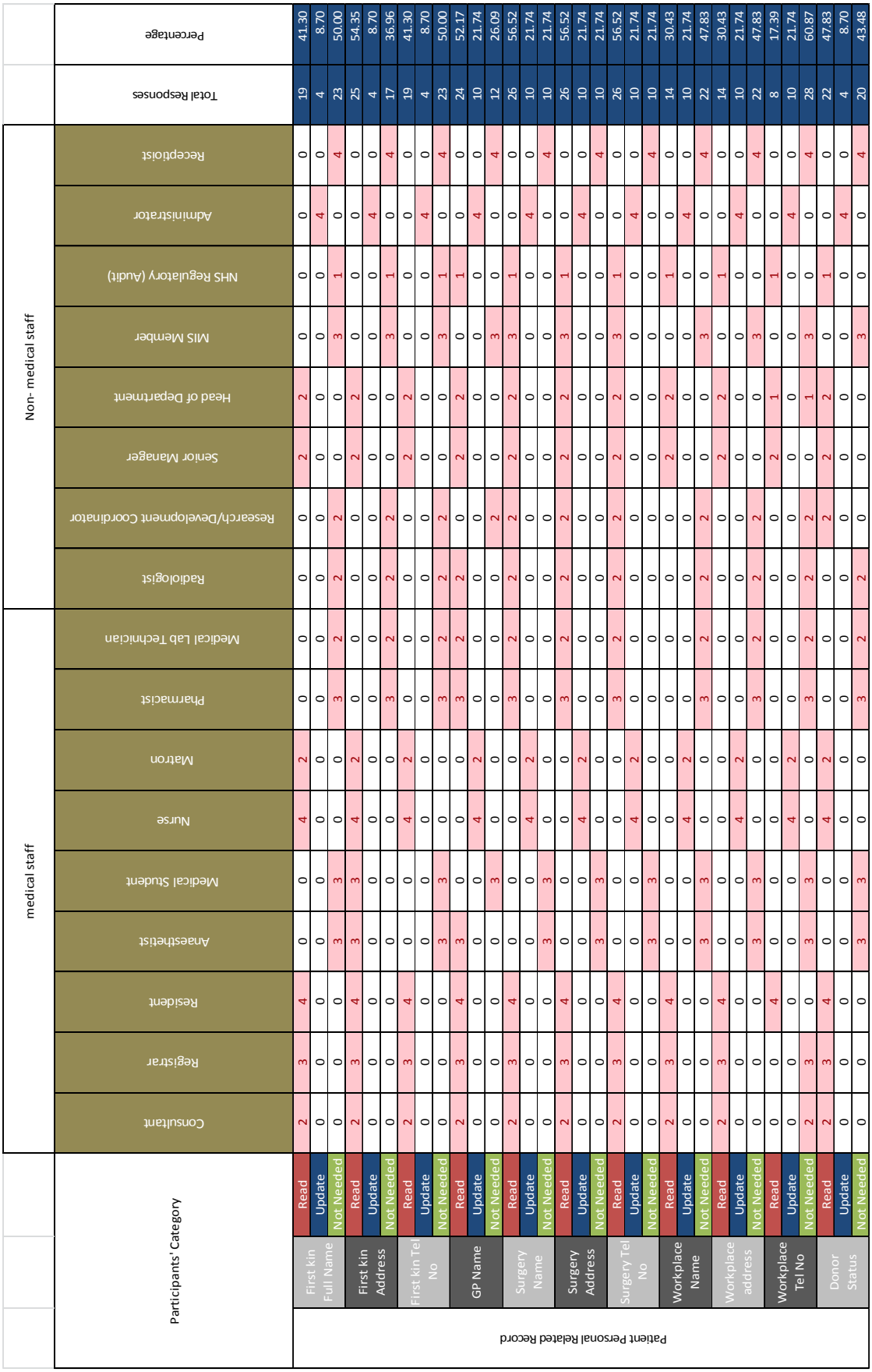
## Patient Related Identity Information

Participants' responses towards patient-related identity information elements are shown in Table 6.4. Consultants', registrars' and residents' responses are the same. They have Read access to all the information apart from consultant and registrars who stated that they do not need the information. The residents also have Read access to workplace telephone number. Heads of department have Read access to all the personal-related information apart from workplace telephone number.

Non-medical staff ,such as pharmacists, medical lab technicians and radiologists have Read access to GP's name, surgery name, surgery address and surgery telephone name. They do not have Read access to the rest of the patient's personal related information. Research/development coordinators indicated that they do not need the vast majority of a patient's related identity information apart from surgery name, surgery address and donor status. MIS members have read only access to the surgery name, address and telephone numbers.

The main aim of this section is to provide in-details patient information. This is needed in healthcare process, identifying the patient, establish information and access control policies.

This section is needed to provide in-details patient related information. This is needed in communication process with patient, patient's kin, work place, GP and surgery (medical centre). The communication needed in facilitating healthcare process and in emergency situation. The EPR structure of this section helps in access control policy, only people who needs the information has access.



| Patient Personal Related Record | Participants' Category | medical staff | | | | | | | | | | | | Non- medical staff | | | | | | | | Total Responses | Percentage |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Consultant | Registrar | Resident | Anaesthetist | Medical Student | Nurse | Matron | Pharmacist | Medical Lab Technician | Radiologist | Research/Development Coordinator | Senior Manager | Head of Department | MIS Member | NHS Regulatory (Audit) | Administrator | Receptionist | | | | | |
| First kin Full Name | Read | 2 | 3 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 2 | 2 | 2 | 3 | 0 | 0 | 0 | | | | 19 | 41.30 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 4 | 8.70 |
| | Not Needed | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 23 | 50.00 |
| First kin Address | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | | | | 25 | 54.35 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 4 | 8.70 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 17 | 36.96 |
| First kin Tel No | Read | 2 | 3 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | | | | 19 | 41.30 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 4 | 8.70 |
| | Not Needed | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 23 | 50.00 |
| GP Name | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | | | | 24 | 52.17 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 10 | 21.74 |
| | Not Needed | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 12 | 26.09 |
| Surgery Name | Read | 2 | 3 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | | | | 26 | 56.52 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 10 | 21.74 |
| | Not Needed | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 10 | 21.74 |
| Surgery Address | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | | | | 26 | 56.52 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 10 | 21.74 |
| | Not Needed | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 10 | 21.74 |
| Surgery Tel No | Read | 2 | 3 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | | | | 26 | 56.52 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 10 | 21.74 |
| | Not Needed | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 10 | 21.74 |
| Workplace Name | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | | | | 26 | 56.52 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 10 | 21.74 |
| | Not Needed | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 10 | 21.74 |
| Workplace address | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | | | | 26 | 56.52 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 10 | 21.74 |
| | Not Needed | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 10 | 21.74 |
| Workplace Tel No | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | | | | 26 | 56.52 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 10 | 21.74 |
| | Not Needed | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 10 | 21.74 |
| Donor Status | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | | | | 26 | 56.52 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 10 | 21.74 |
| | Not Needed | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 10 | 21.74 |
| | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | | | | 26 | 56.52 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 10 | 21.74 |
| | Not Needed | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 10 | 21.74 |
| | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | | | | 10 | 21.74 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 4 | 8.70 |
| | Not Needed | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 20 | 43.48 |

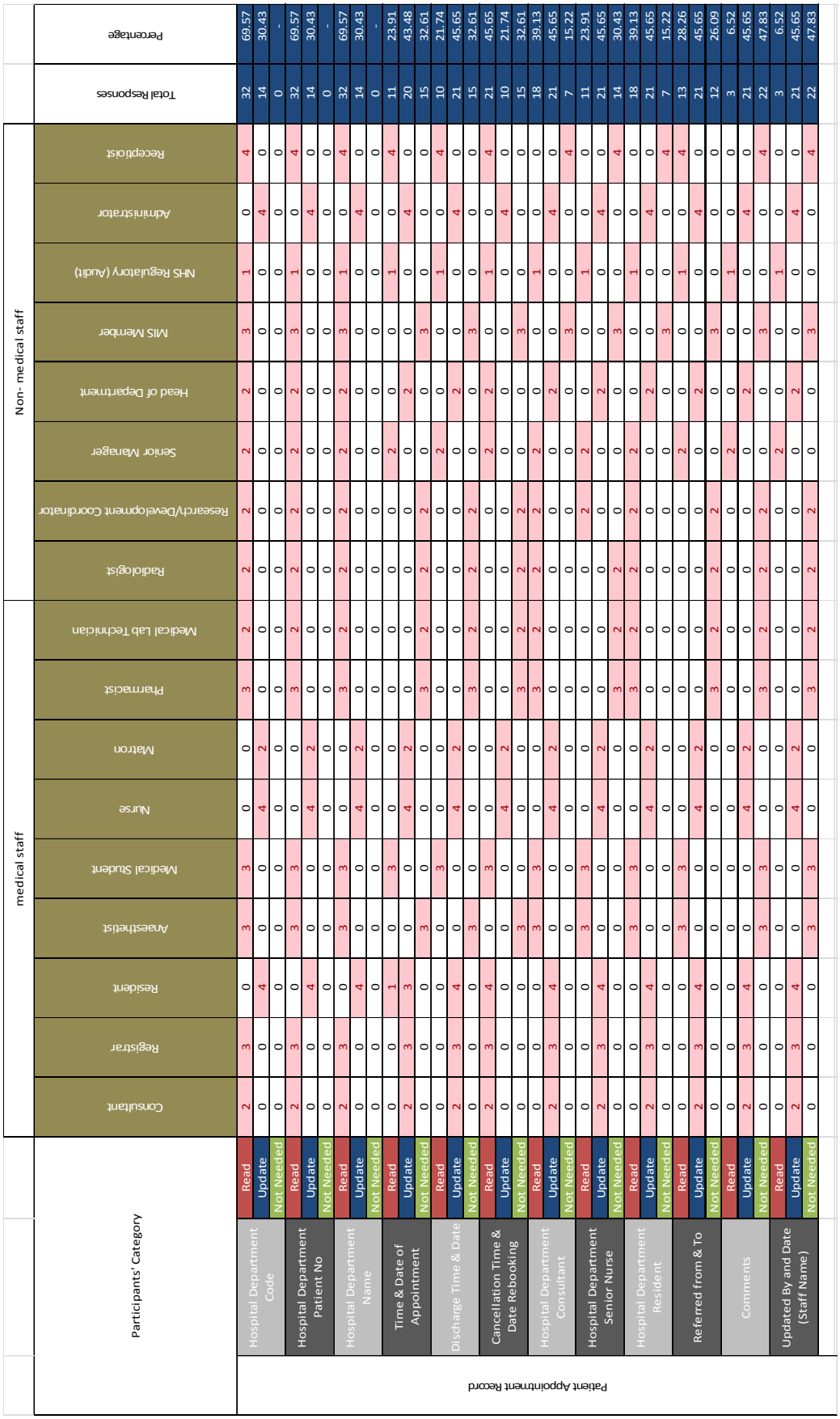
**Table 6-4 : Patient Related Identity Information**

## Patient Appointment Record

The data analysis showed that the consultants, registrars and head of department have similar access privilege, (see Table 6.5). They have Update access to the vast majority of the information and have Read access to the hospital department code, patient number, department name, cancellation time and rebooking, and cancellation date. Residents have similar access apart from having Update access to hospital department code, patient number, name, date and time of appointment. The results also indicated that the nurse and matrons have the same privilege. They have Update access to all the items in the patients' appointment record. Anaesthetists have Read access to hospital department code, patient number, name, consultant name, senior nurse name, resident's name, referral from, and referred to information. They indicated that they do not have to access the information for the rest of the appointments.

Non-medical staff pharmacists, medical lab technicians, and radiologists indicated that they have similar Read access to hospital department code, patient number, department name. The rest of the respondents indicated that they do not have access to the information. The administrator indicated that they have Update access to all the patient appointment record items. On the other hand, the receptionists indicated that they have Read access to the record items, apart from consultant name, senior name in charge, and resident in charge name, add comments and signing and dating the record. On the other hand, MIS members indicated that they do not have access to the record items apart from hospital department code, hospital department patient number, and hospital department name to which they have Read access.

The main aim of this section is to provide in-details patient information. This is needed in healthcare process, identifying the patient, establish information and access control policies.



| | Participants' Category | medical staff | | | | | | | | | | | | Non- medical staff | | | | | | | | Total Responses | Percentage |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Consultant | Registrar | Resident | Anaesthetist | Medical Student | Nurse | Matron | Pharmacist | Medical Lab Technician | Radiologist | Research/Development Coordinator | Senior Manager | Head of Department | MIS Member | NHS Regulatory (Audit) | Administrator | Receptionist | | | | | |
| Patient Appointment Record | Hospital Department Code | 2 | 3 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 2 | 2 | 3 | 1 | 0 | 4 | | | | 32 | 69.57 |
| | | 0 | 0 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 14 | 30.43 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | 0 | - |
| | Hospital Department Patient No | 2 | 3 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 2 | 2 | 3 | 1 | 0 | 4 | | | | 32 | 69.57 |
| | | 0 | 0 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 14 | 30.43 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | 0 | - |
| | Hospital Department Name | 2 | 3 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 2 | 2 | 3 | 1 | 0 | 4 | | | | 32 | 69.57 |
| | | 0 | 0 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 14 | 30.43 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | 0 | - |
| | Time & Date of Appointment | 2 | 3 | 3 | 0 | 0 | 4 | 2 | 0 | 2 | 2 | 2 | 2 | 2 | 0 | 0 | 4 | 0 | | | | 11 | 23.91 |
| | | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 20 | 43.48 |
| | | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 15 | 32.61 |
| | Discharge Time & Date | 2 | 3 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 1 | 0 | 4 | | | | 10 | 21.74 |
| | | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 21 | 45.65 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 15 | 32.61 |
| | Cancellation Time & Date Rebooking | 2 | 3 | 4 | 0 | 3 | 0 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 3 | 1 | 0 | 4 | | | | 21 | 45.65 |
| | | 0 | 0 | 0 | 3 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 10 | 21.74 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 2 | 2 | 0 | 0 | 3 | 1 | 0 | 0 | | | | 15 | 32.61 |
| | Hospital Department Consultant | 2 | 3 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | | | | 18 | 39.13 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 4 | | | | 21 | 45.65 |
| | | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 2 | 2 | 0 | 1 | 0 | 0 | | | | 7 | 15.22 |
| | Hospital Department Senior Nurse | 2 | 3 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 11 | 23.91 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | 21 | 45.65 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 2 | 2 | 2 | 2 | 3 | 1 | 0 | 4 | | | | 14 | 30.43 |
| | Hospital Department Resident | 2 | 3 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 18 | 39.13 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | 21 | 45.65 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 4 | | | | 7 | 15.22 |
| | Referred from & To | 2 | 3 | 4 | 0 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 1 | 0 | 4 | | | | 13 | 28.26 |
| | | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | 21 | 45.65 |
| | | 0 | 0 | 0 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | | | | 12 | 26.09 |
| | Comments | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 2 | 2 | 2 | 0 | 3 | 1 | 0 | 4 | | | | 3 | 6.52 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | | | | 21 | 45.65 |
| | | 2 | 3 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | | | | 22 | 47.83 |
| | Updated By and Date (Staff Name) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 2 | 2 | 2 | 0 | 3 | 1 | 0 | 4 | | | | 3 | 6.52 |
| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | | | | 21 | 45.65 |
| | | 2 | 3 | 4 | 0 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 1 | 0 | 4 | | | | 22 | 47.83 |
| | | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 2 | 0 | 3 | 1 | 0 | 4 | | | | | |

**Table 6-5 : Patient Appointment Record**

## Non-medical Information

The data analysis showed that consultants and registrars have the same access. They have Read access to the non-clinical information and Update access to the name of the consultant in charge of the patient's care, resident name and the senior name. The residents indicated that they have Update access to the non-clinical information record. Anaesthetists and medical students have Read only access to the record. Hospital nurses and matrons have Update access to all the non-clinical information record (see Table 6.6).

Lab technicians and the radiologists have the same Read access to the record. They have Read access to the hospital name, hospital address, hospital telephone number, ward number, bed number, and name of consultant in charge, resident in charge. They expressed that they do not have access to the name of the senior nurse in charge. Administrators have Update access to the record while the receptionists have only Read access to the record and do not have access to the names of the consultant, residents, or senior nurse in charge.

The main aim of this section is needed to establish policy and access control. Only people who needs this type of information should have access to this section.

| Non-Clinical Information | Participants' Category | medical staff | | | | | | | | | | | Non- medical staff | | | | | | | | | | | | Total Responses | Percentage |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Consultant | Registrar | Resident | Anaesthetist | Medical Student | Nurse | Matron | Pharmacist | Medical Lab Technician | Radiologist | Research/Development Coordinator | Senior Manager | Head of Department | MIS Member | NHS Regulatory (Audit) | Administrator | Receptionist | | |
| Hospital Name | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 0 | 1 | 0 | 4 | 39 | 84.78 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 4 | 0 | 7 | 15.22 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - |
| Hospital Address | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 0 | 1 | 0 | 4 | 39 | 84.78 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 4 | 0 | 7 | 15.22 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - |
| Hospital Telephone Number. | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 0 | 1 | 0 | 4 | 39 | 84.78 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 4 | 0 | 7 | 15.22 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - |
| Ward Number | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 0 | 1 | 0 | 4 | 27 | 58.70 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 4 | 0 | 16 | 34.78 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 6.52 |
| Room Number | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 0 | 1 | 0 | 4 | 27 | 58.70 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 4 | 0 | 16 | 34.78 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 6.52 |
| Bed Number | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 0 | 1 | 0 | 4 | 27 | 58.70 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 4 | 0 | 16 | 34.78 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 6.52 |
| Consultant in patient care Charge Name | Read | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 18 | 39.13 |
| | Update | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | 21 | 45.65 |
| | Not Needed | 2 | 3 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | 7 | 15.22 |
| Physician/Resident in Charge Name | Read | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 4 | 11 | 23.91 |
| | Update | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 3 | 2 | 2 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | 21 | 45.65 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | 14 | 30.43 |
| Senior Nurse in Charge Name | Read | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 0 | 1 | 0 | 4 | 27 | 58.70 |
| | Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 4 | 0 | 16 | 34.78 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 6.52 |

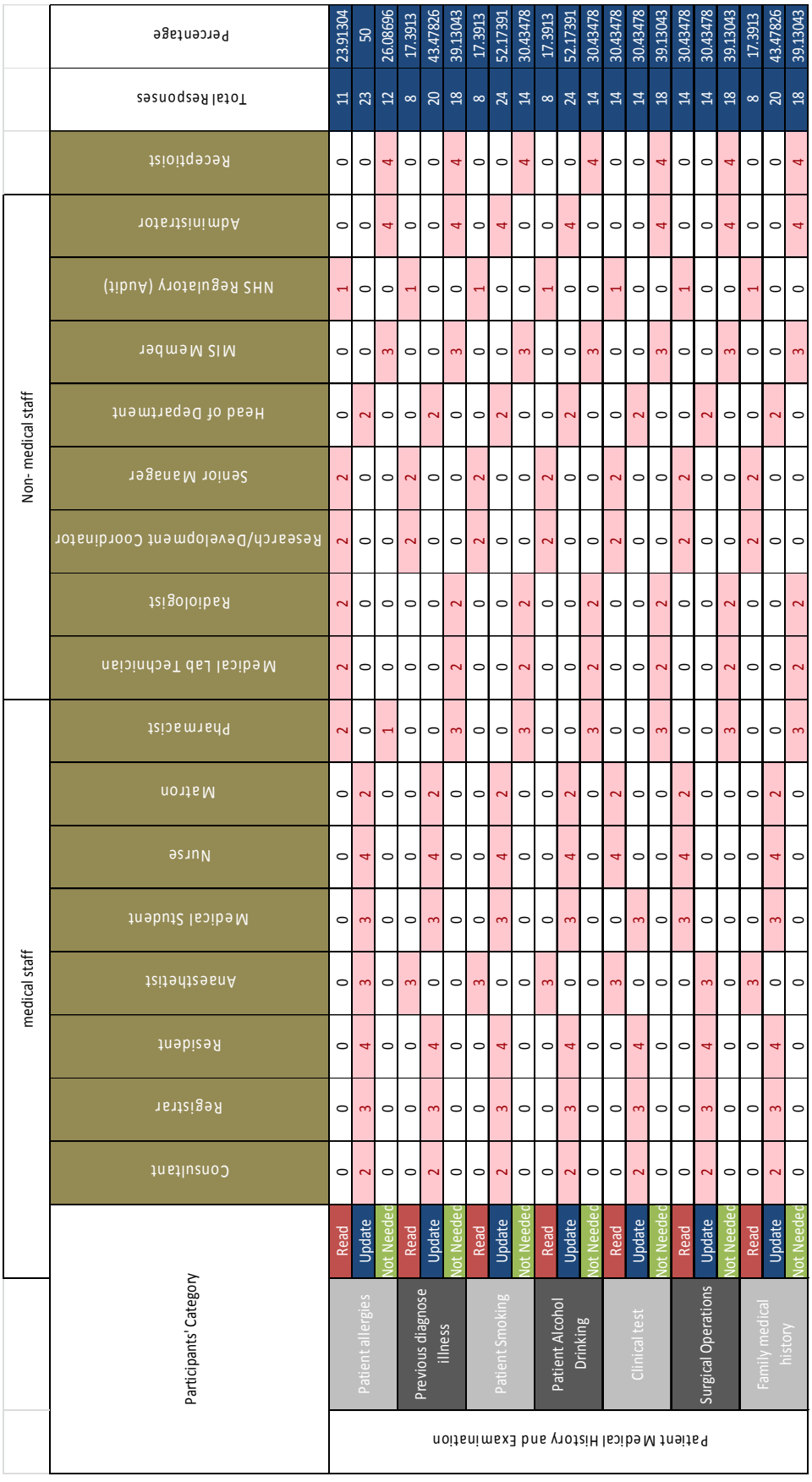
**Table 6-6 : Non-clinical Information**

## Patients Medical History and Examination

Table 6.7 shows the participants' responses towards patient's medical history and examination. The table shows that consultants, registrars, residents and heads of departments have Update access to the patient medical history and examination record. Nurses and the matrons have similar access to the record. They indicated that they have Update access to the records items and Read access to the clinical tests and surgical operations. Anaesthetists have Update access to the information and have Read only access to the previously diagnosed illness, patient smoking, alcohol drinking, clinical tests, and family medical history. Medical students have Update access and Read only access to the surgical operations item.

For non-clinical staff, medical lab technicians and radiologists indicated that they do not have access to the record apart from the patients' allergies (Table 7.6). Administrators indicated that they do not have access to the record apart from Read access to the patient's smoking and alcohol habits. Receptionists and MIS members indicated that they do not have access to the record while the NHS regulatory indicated they have Read access to the record items.

This section provides in-details patient's medical history and examination. This is needed in healthcare process and in establish information and access control policies,

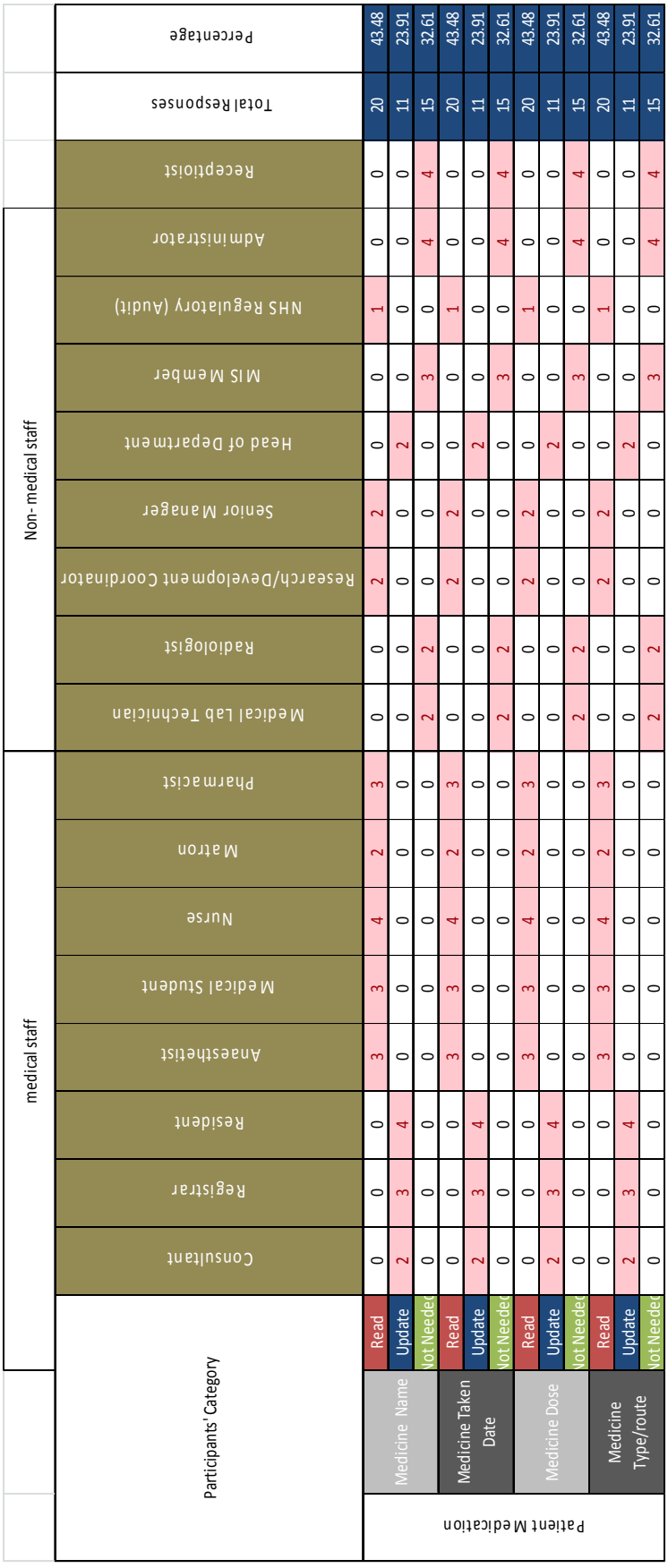


| Patient Medical History and Examination | Participants' Category | medical staff | | | | | | | | | | Non- medical staff | | | | | | | | | | Total Responses | Percentage |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Consultant | Registrar | Resident | Anaesthetist | Medical Student | Nurse | Matron | Pharmacist | Medical Lab Technician | Radiologist | Research/Development Coordinator | Senior Manager | Head of Department | MIS Member | NHS Regulatory (Audit) | Administrator | Receptionist | | | | | |
| Patient allergies | Read | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | | | | 11 | 23.91304 |
| | Update | 2 | 3 | 4 | 3 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 3 | 0 | 0 | 0 | | | | 23 | 50 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 4 | | | | 12 | 26.08696 |
| Previous diagnose illness | Read | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | | | | 8 | 17.3913 |
| | Update | 2 | 3 | 4 | 0 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 3 | 0 | 0 | 0 | | | | 20 | 43.47826 |
| | Not Needed | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 4 | | | | 18 | 39.13043 |
| Patient Smoking | Read | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | | | | 8 | 17.3913 |
| | Update | 2 | 3 | 4 | 0 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | | | | 24 | 52.17391 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 2 | 0 | 0 | 0 | 3 | 0 | 0 | 4 | | | | 14 | 30.43478 |
| Patient Alcohol Drinking | Read | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | | | | 8 | 17.3913 |
| | Update | 2 | 3 | 4 | 0 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | | | | 24 | 52.17391 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 2 | 0 | 0 | 0 | 3 | 0 | 0 | 4 | | | | 14 | 30.43478 |
| Clinical test | Read | 0 | 0 | 0 | 3 | 0 | 4 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | | | | 14 | 30.43478 |
| | Update | 2 | 3 | 4 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | | | | 14 | 30.43478 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 2 | 0 | 0 | 0 | 3 | 0 | 0 | 4 | | | | 18 | 39.13043 |
| Surgical Operations | Read | 0 | 0 | 0 | 3 | 0 | 4 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | | | | 14 | 30.43478 |
| | Update | 2 | 3 | 4 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | | | | 14 | 30.43478 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 2 | 0 | 0 | 0 | 3 | 0 | 0 | 4 | | | | 18 | 39.13043 |
| Family medical history | Read | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | | | | 8 | 17.3913 |
| | Update | 2 | 3 | 4 | 0 | 3 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | | | | 20 | 43.47826 |
| | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 2 | 0 | 0 | 0 | 3 | 0 | 0 | 4 | | | | 18 | 39.13043 |

**Table 6-7 : Patients Medical History and Examination**

## Patients Medication

Consultants, registrars, residents and heads of departments have Update access to the patients' medication record. The rest of the medical staff, anaesthetists, medical students, nurse and matron have Read Only access. Non-medical staff medical lab technicians, radiologists' administrators, receptionists, MIS members, have no access to the medication information record. On the other hand, pharmacists, senior managers, research/development coordinators and NHS regulators have Read access (see Table 6.8). The main aim of this section is to provide in-details patient medication. This is needed in the patient's healthcare process, identifying, establish information and access control policies.



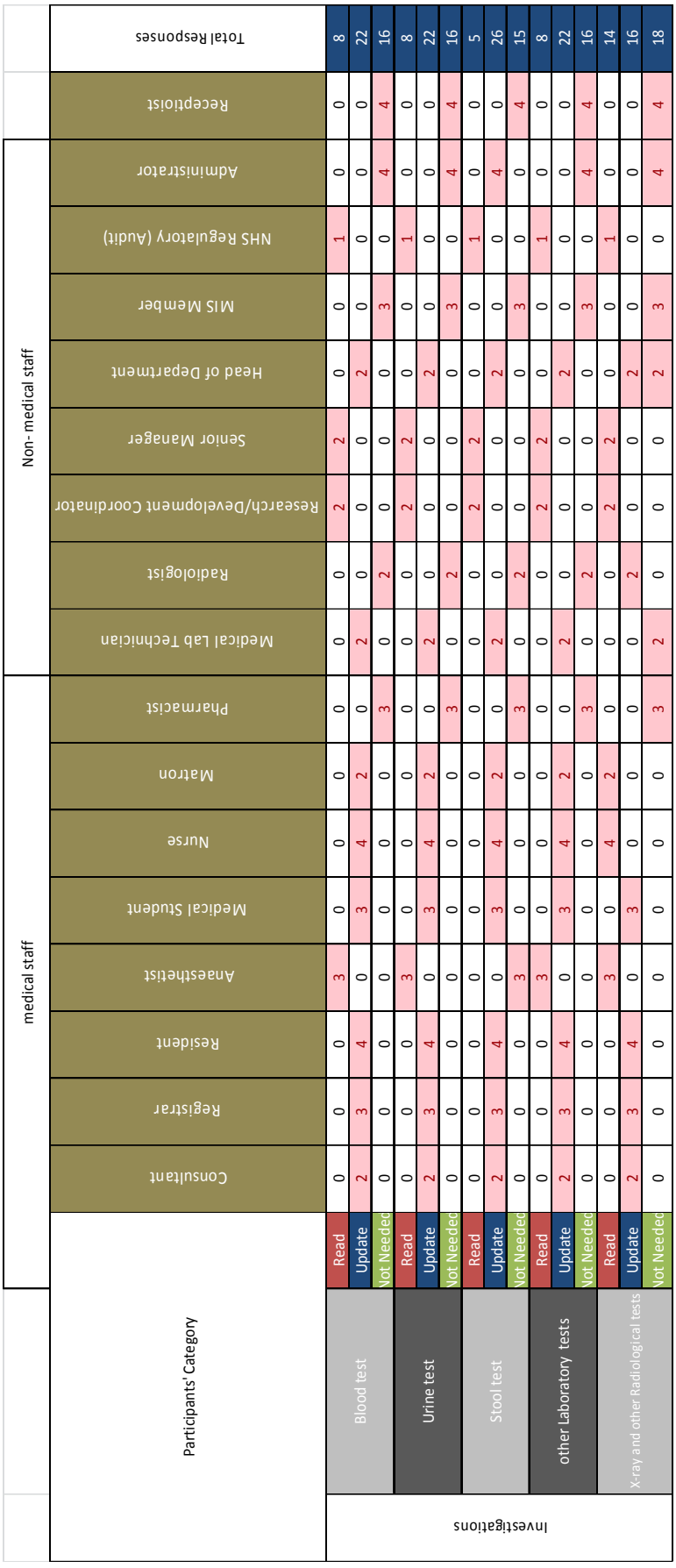
| | Participants' Category | Consultant | Registrar | Resident | Anaesthetist | Medical Student | Nurse | Matron | Pharmacist | Medical Lab Technician | Radiologist | Research/Development Coordinator | Senior Manager | Head of Department | MIS Member | NHS Regulatory (Audit) | Administrator | Receptionist | Total Responses | Percentage |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Patient Medication | Medicine Name | Read | 0 | 0 | 0 | 3 | 3 | 4 | 2 | 3 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | 20 | 43.48 |
| | | Update | 2 | 3 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 11 | 23.91 |
| | | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 3 | 0 | 0 | 4 | 15 | 32.61 |
| | Medicine Taken Date | Read | 0 | 0 | 0 | 3 | 3 | 4 | 2 | 3 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | 20 | 43.48 |
| | | Update | 2 | 3 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 11 | 23.91 |
| | | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 3 | 0 | 0 | 4 | 15 | 32.61 |
| | Medicine Dose | Read | 0 | 0 | 0 | 3 | 3 | 4 | 2 | 3 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | 20 | 43.48 |
| | | Update | 2 | 3 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 11 | 23.91 |
| | | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 3 | 0 | 0 | 4 | 15 | 32.61 |
| | Medicine Type/route | Read | 0 | 0 | 0 | 3 | 3 | 4 | 2 | 3 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | 20 | 43.48 |
| | | Update | 2 | 3 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 11 | 23.91 |
| | | Not Needed | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 3 | 0 | 0 | 4 | 15 | 32.61 |

**Table 6-8 : Patients Medication**

## Investigation Record

The patient's investigation record includes blood test, urine test, stool test, x-ray and other radiological tests, and other laboratory tests. Table 6.9 shows the responses towards the investigation record. The analysis indicated that consultants, registrars, residents' head of department and medical students have Update access to the investigations record. Anaesthetists have Read access to the blood test and to urine tests apart from the stool test. Hospital nurses and matrons have Read access to the investigation record.

Administrators, MIS members and receptionists do not have access to the information record. Radiologists indicated that they have Update access only in the x-ray and other radiological tests. Medical lab technicians have Update access to the record apart from the x-ray and other radiological tests. NHS regulatory and research/development coordinators have Read access to the investigation record. Finally, pharmacists indicated that they have no access to the record. This section is needed in patient's healthcare process, establish information and access control policies.



| | Participants' Category | Consultant | Registrar | Resident | Anaesthetist | Medical Student | Nurse | Matron | Pharmacist | Medical Lab Technician | Radiologist | Research/Development Coordinator | Senior Manager | Head of Department | MIS Member | NHS Regulatory (Audit) | Administrator | Receptionist | Total Responses |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Investigations | Blood test | Read 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | 8 |
| | | Update 2 | 3 | 4 | 0 | 3 | 4 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 22 |
| | | Not Needed 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 2 | 0 | 0 | 0 | 3 | 0 | 4 | 4 | 16 |
| | Urine test | Read 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 8 |
| | | Update 2 | 3 | 4 | 0 | 3 | 4 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 22 |
| | | Not Needed 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 2 | 0 | 0 | 0 | 3 | 1 | 4 | 4 | 16 |
| | Stool test | Read 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | 5 |
| | | Update 2 | 3 | 4 | 0 | 3 | 4 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | 26 |
| | | Not Needed 0 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 2 | 0 | 0 | 0 | 3 | 0 | 0 | 4 | 15 |
| | other Laboratory tests | Read 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | 8 |
| | | Update 2 | 3 | 4 | 0 | 3 | 4 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 22 |
| | | Not Needed 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 2 | 0 | 0 | 0 | 3 | 0 | 4 | 4 | 16 |
| | X-ray and other Radiological tests | Read 0 | 0 | 0 | 3 | 0 | 4 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | 14 |
| | | Update 2 | 3 | 4 | 0 | 3 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 16 |
| | | Not Needed 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 0 | 0 | 0 | 2 | 3 | 0 | 4 | 4 | 18 |

**Table 6-9 : Investigations Record**

## 6.3 Policy Matrix

The core of this research is the analysis of the EPR information security policy. The research found that there is no clear and detailed information security for EPR in the surveyed hospital. The policy document is brief and generic. The research failed to find specific EPR information within the policy to protect the patient identity from any misuse of the information. Therefore, the research stresses the importance of and need for analysing and establishing such a policy. Hospital policy regarding patients' personal information does not exist. There is no statement within the policy indicating access control of the information based on the medical and non-medical staff's needs. The policy does not recognise type and sensitivity of information within the EPR. The hospital policy lacks any statement regarding the hospital staff's responsibilities to such information and the consequences of not complying with the policy. The patient's identity-related information has no policy assigned to the users based on their needs and responsibilities. There is a need for such an information policy to identify responsibility and to ensure information security.

It is difficult to find a clear policy for accessing patient appointment records and stipulating the consequences of failing to comply with such information. Although the hospital gave permission to certain staff to access and/or update patients' appointment records, there is no policy for the control of such information.

Patients' medical history and examination information is sensitive and confidential information from the patients' point of view as well as from the hospital's. The hospital information security policy fell short of establishing policy for EPR. There is no access control policy stipulating the consequences of breaking such information. There is an urgent need to establish such a policy in order to ensure security of such information. The hospital policy also has no policy statements that show the access control of patients' medication. Although the system recognises the access of such information and gives privileges to certain staff to update and read such information, the hospital has no policy defining and giving privilege access and update access to the information. There is a need to establish policy regarding patient medication access. This can be achieved by providing a clear access control policy.

The current access control policy is based on access to the information system without any restriction or control. The analysis of hospital policy indicated that the policy focuses mainly on setting the *Username* and *Password* for the system users and validating the setting and process they need to follow to applying for new ones. This means that the policy does not reflect the real needs of the organisation. The main problem in the current access control policy is that the policy treats all users the same. The system has one level of security without any consideration of the value and type of information in the system. Once the user has obtained a username and password from the hospital's ICT team, they have access to the system regardless of the user's information needs.

The policy states that the user's needs have to meet the requirements of the access management to avoid any suspension. However, the policy and its attachment do not give the details of these requirements and the consequences of not complying with the requirements. However, the requirements are mainly:

> "*All users should meet the requirements of the access management system to avoid the suspension of their account privileges to the hospital systems*"
> (KFH Information Policy, 2010).

The access control policy is mainly concerned with terminating employees' access to the systems and with termination of their account. The policy defined the condition that employee access to the hospital electronic system will be terminated in the event of an employee's employment with the hospital finishing. The policy stated in this regard:

> "*An employee is permanently leaving the hospital (retired, resigned, not eligible for hiring, etc ...)*".
> (KFH Information Policy, 2010).

The above policy is mainly concerned with not allowing non-employed subjects to access their information systems. The policy is clear in seizing the access rights of an employee once his or her relations with the hospital are completed. However, the hospital does not state any policy during an employee's term of employment. In other words, the current policy fails to protect and secure information from current employees; and trusts the employees regardless of their profession, information needs, cultural issues, awareness and understanding of the importance of information security.

The other concern of the current access control policy is that the system fails to distinguish category between types of users. The access control policy does not recognise the differences in employees' job roles and responsibilities. There are several professions which play a role in patient care in the hospital working environment, such as medical consultants, physicians and nurses as example. The policy needs to distinguish between these professions and build a policy based on the professions' information needs. This helps to protect and secure the information.

### 6.3.1 Suspension Policy

Suspension of access to the hospital system is mainly concerned with denying access to the system and mainly targets employees who have completed their contract with the hospital. It seems that the policy does not consider information security beyond employees with terminated contracts. The main concern is that the policy does not treat the EPR and other hospital information with the privilege it deserves from a confidentiality and security point of view. The hospital policy in this regard stated:

- "*In case of suspension, user account will be disabled immediately*".
- "*A notification email will be sent to the user and to his/her supervisor according to HR hierarchy*".

The suspension of hospital access falls short on passing the appropriate message to the abuser of the system and the rest of the hospital EPR users. The suspension lacks a process of investigating the main reasons for suspensions. The main concern of the hospital should be to focus on avoiding any repetition of any similar cases of abuse of EPR information. This can be achieved by investigating thoroughly and identifying the

main reasons for the abuse. This may require the policy to be modified to include a statement that enhances the current policy. There is also a need for a clear policy for consequences of abusing the system. This needs to go beyond suspension from accessing the system and may need to include more serious consequences.

#### *6.3.1.1 Policy Establishment Process*

One of the main concerns of the hospital is the lack of a process for formulating effective information security policy. It is important to stress that information security is a dynamic issue. This is due to changes in the technology used in the information security system and changes in employees and their positions at the SA NHS. It is important to establish a clear strategy of a policy formulating process. The following should to be taken into account:

- Involve most of the EPR stakeholders including the patient. This is needed to express their views and opinions towards establishing an effective information security policy.
- Take advantage of the knowledge and experience of other organisations in information security; consider what is most useful for the hospital, especially developments in Western countries.
- Reflect on the experience and knowledge gained by the hospital in information security. This may include reflecting on any EPR information security issues explored or identified such as abuse of the system's investigation by internal or external users.
- Use of technology development to enhance the hospital information security, protecting the information. This should include the use of hardware and software.
- Review the current system and its impact on the EPR information security. The system needs to be reviewed regularly in order to ensure the EPR information security. This is mainly due to changes in technology and possibly hackers developing new tools with which to abuse the system.
- Review the current policy and reflect on its effectiveness in enforcing the policy and its robustness and effectiveness for protecting EPR.

- Involve the hospital staff in the EPR information policy formulation process to use their experience and knowledge in the issue. From management point of view, it is also important to ensure that the staff feel that they are part of the process. This helps in the implementation and enforcement of the policy.

## 6.4 Summary

The evaluation indicated that the analysis of the EPR security policy reflects the needs and reality of the organisation. The evaluation indicated that access to the EPR is not controlled and managed based on the users' roles in the patient care process. The evaluation identified each profession in the SA-NHS services types of information they need for their role in the patient health care process. The evaluation also indicated that there is a mismatch between the stated policy and the organisation practices. The policy does not reflect organisational reality and the actual working practices in the organisation. The evaluation process used to check the usefulness, reliability and practicality of the EPR model as several subjects from different professions used in the process and different resources used to reach the main outcomes of the evaluation. The outcomes of the evaluation aimed to answer the research questions by evaluating the EPR security policy and verifying its translation into organisational reality. The outcomes of this research will be used as a focus for the research discussion. This will be presented in the next chapter, Chapter 7.

# CHAPTER SEVEN:

# DISCUSSION

Objectives

- To discuss the current situation of EPR in SA
- To discuss and evaluate the developed EPR model
- To discuss EPR Information Security Policy
- To discuss SA Health Service EPR Policy

# 7 CHAPTER SEVEN: DISCUSSION

## 7.1 Introduction

This chapter presents and discusses the main outcomes of this research. This includes discussions of the current situation of the use of EPR in the SA NHS. The discussions include patients' rights towards their EPR record, patients' consent and EPR ownership. The discussion then focuses on the current EPR system in the surveyed hospital. The research also discusses the main risks of implementing EPR in the SA NHS, followed by the development and evaluation of EPR. EPR information security and access control policy are presented and discussed in this chapter. The chapter closes with the main barriers and obstacles to EPR adaptation in the SA NHS.

## 7.2 Current Situation of EPR in SA

One of the main objectives of this research is to "Investigate the current situation of electronic patient record in Saudi Arabia." Investigating the current situation helps to identify the current EPR system usage and EPR security practices in the SA NHS and to determine what needs to be changed in order to enhance and promote EPR security within the services. The first step of the research investigated the current situation of the EPR system used and of EPR security practices in the SA NHS. This section presents and discusses the current situation based on the outcomes of the qualitative and quantitative data collected during the research process and the document analysis.

### 7.2.1 Patient Rights

One of the main outcomes of this research is the SA NHS patient's rights access to his/her EPR record. SA NHS employees agreed that the patient has a right to access his/her EPR. Although this right is clearly expressed, there is little evidence that the SA NHS health services policies reflect or promote this right. The following are the main issues identified in this research regarding the SA NHS patients' rights.

It is also important to stress that providing patients with their own EPR online creates new requirements to ensure protection of the data privacy and access control (Sujansky et al., 2010). The SA NHS needs to take such a problem into consideration.

#### *7.2.1.1 Patient's Consent*

The document analysis and the interviews indicated the SA NHS' lack of electronic and non-electronic patient consent process and procedure for patients to consent to give permission to a third party to access part of or the whole of the EPR record. Currently the SA NHS lacks any form of patient consent to protect and enhance the patient's right. The patient's consent is needed to give the SA NHS the right to manage, transfer, and access patient information to any of the patient's stakeholders such as the policy, social services as examples. The SA NHS currently has a serious challenge and problems in handling and passing EPR information without the patient's consent. This has serious moral and legislation consequences. The main problem currently identified is the lack of patient and staff awareness of the need for such an important patient's form. In summary, there is a difference between the belief that the patient has the right to his/her patient record and the actual practices. From the belief point of view, the data analysis indicated that the hospital staff, including the managers, believe and understand the patient's rights towards their EPR. However, from the practical point of view, there is no evidence for translating such beliefs into organisational reality. There is no clear evidence in the hospital policy indicating either the patient's rights or the existence of a form for patient's consent. This may be due to a lack of knowledge and experience in information security policy or to the hospital's priority at this stage. This study reveals that there is a lack of staff awareness towards the patient's right to access their EPR record and the need of such right to be implemented in the actual practices within the services regarding this right.

#### *7.2.1.2 EPR Ownership*

The current situation regarding EPR ownership is still not clear within SA NHS. There are a large number of people within the SA NHS who believe that the patient is the sole owner of the EPR. However, there are people within the SA NHS who believe that the EPR owner is the NHS organization, SA NHS, and not the patient. The medical staff are mainly the subjects who believed that the patient is the owner of the EPR record. On the other hand, hospital managers and administrators are mainly the subjects who believe that the SA NHS is the sole owner of the EPR record.

This diversity in the opinions towards the EPR ownership may lead to a delay in formulating appropriate policy for protecting EPR information security. One of the main problems for this difference is the lack of policy that stresses ownership of the EPR and processes for managing the EPR records. For this reason, this research strongly stresses the need for establishing such a policy.

### 7.2.2 Current System Used by the Hospital

The ICT personnel indicated clearly that they have introduced an EPR system as part of the KFH ICT strategy. SA NHS and the Saudi market fell short of developing and designing EPR systems that meet the SA NHS needs and specifications due to a lack of technical knowledge and experience in developing EPR systems. The SA NHS option was to take advantage of developed country experience and knowledge in this area due to the lack of expertise in this area in SA. The SA NHS bought a system from a US company as part of a contract with the SA NHS. The EPR system was installed and used by the hospital staff as part of the hospital strategy to improve the hospital performance and care system within the hospital. A group of selected staff were trained in the USA in using the system in order to promote the staff's knowledge, skills and competence in using the system as well as to be a core for training the rest of the hospital staff, as part of a "*train the trainer*" scheme.

#### *7.2.2.1 The Current Use of the System*

The current system is used by most of the hospital staff, particularly the hospital medical staff in the patients' care process of the hospital. One of the main concerns of the system is that the hospital denied patients access to their own personal EPR record. The current patients are aware of the use of EPR in their care process but they never used or closely examined the system. This is due to a lack of strategy and awareness of the hospital management in giving the patients the right to access their own EPR. Therefore, the hospital needs to establish a strategy and policy towards the patients' right to access their EPR record. The current use of the system is based on the localized hospital without any link of the system to other hospitals within the SA NHS network of hospitals and medical centres.

#### *7.2.2.2 The Current Information Security Policy in SA-NHS*

Currently the hospital has a brief and generic policy regarding EPR security. The hospital has an information security policy document (see Appendix 3). This document is distributed to the medical staff regarding the use of ICT within the hospital. The policy is generic without any clear guidelines and statements. The interviewees believed that the hospital has an EPR security policy. They stressed that all the hospital staff are given a copy of the hospital security policy. However, the physician stressed that the policy falls short of meeting the standard required to protect the EPR. The physician also stressed the need to improve and update the current policy due to changes in patient rights and so as to avoid any unauthorised access to the EPR. The main concern was that the policy does not have any guidelines to control access to EPR based on the users' information needs.

The current policy is not clear and this has led to several concerns and the need for clarifications. For this reason, the hospital nominated a member of staff from each hospital profession and department to respond to any information security enquiries. The nomination of the staff is based on their experience and knowledge of information security. They are usually trained in the system and in the SA-NHS security policy. Each nominated staff member will be responsible for providing advice and clarification to his/her department staff. In case the nominated staff member needs policy clarification, he/she needs to contact the hospital senior management as they are the main decision makers in security policy due to the hospital management structure and responsibilities. This leads to state the SA NHS is highly based on a subjective approach, personal based decisions. The information security policy passed through the hospital structure verbally as understood by the individuals within the system. There are several problems in adopting such an approach. These problems include:

(i) <u>difficult to trace the policy,</u>

One of the main critical difficulties identified is tracing the EPR information security policy. The hospital staff, as well as EPR stakeholder, found difficulties in tracing the EPR policy. The tracing difficulty can be divided into two areas. Firstly, identifying the location of the policy and secondly, tracing policy regarding the EPR security statements within the policy.

(ii) different interpretation of the policy, subjective;

Most of the information policy is generic and does not concentrate on access control to the EPR. This has led to several situations where information security issues were raised by the staff. The current policy statements are unclear and do not cover the vast majority of information security issues. The current reality of the policy is that staff use their own interpretation of the policy and act based on their own knowledge and experience through subjective interpretation.

(iii) takes time and effort to find the appropriate subject;

There are relatively few members of staff who have been trained on the EPR system and trained in the US on the system and on security issues. One of the main current difficulties facing the staff is finding the right person to answer or explain their EPR information security enquiry. It takes time and effort to identify the experienced, knowledgeable and authoritative individual within the system to clarify issues or make decisions on an EPR information security issue. It can be argued that the organisation's centralised management system further affects the issue, since there are few people with the courage to make decisions or to interpret information security as it is difficult for individuals to take the risk of conflict with the hospital senior management.

(iv) Difficulties in accessing the right information at appropriate time and place;

The vast majority of the SA NHS are relatively large hospitals with several departments and there are hospitals with several branches. One of the difficulties is that the departments within the hospitals have no access to information security at their department and they cannot find appropriate information that is specifically written to meet their departmental activities.

(v) subjective in consequences for not complying with the information security policy:

One of the main current difficulties of the current policy is the consequences of any abuse to the EPR information security by internal or external abuser. The current policy stresses mainly on denying any abuse and access to the system. This is not clear in the current policy and the vast majority of the

decisions are currently based on management decisions. There is a need for robust information security with clear consequences for any abuse of the EPR system to protect the patient's privacy and the integrity of the medical information.

### 7.2.3 Main Risk for Implementing EPR in SA-NHS

Implementing EPR systems in SA NHS has several risks. These risks are mainly due to the fact that the SA NHS is in a transition period, shifting from a traditional paper based recording system to electronic recording. The transition period requires changes in two main elements of the SA NHS. The first element is change in the organization culture and the second is change in using technology in handling and managing patients' records. Each of the elements has its own associated risks. It is critical to identify the current main risks to the SA NHS to help in eliminating such risks from the hospital processes to protect EPR. This research explored several current risks to information security within SA-NHS. These risks can be classified into cultural issues and technological issues.

#### *7.2.3.1 SA NHS Organization Culture Risks*

Shifting from traditional recording to an electronic record requires changes in the SA NHS staff's information seeking behaviour and their daily practices. The change requires staff to use electronic tools to seek medical information, such as use of a medical database to find appropriate medicine. This is a totally different approach from the traditional approach of using hardcopy indices and medical abstracts. It can be argued that changing the people should go hand in hand with changing the technology. It is not a major issue for the SA NHS authority to buy in a new technology system to support the services operations. The SA NHS is a public service managed and backed by the SA central government. The real challenge remains in consistency of the staff to accept the change. The staff change focuses on staff being willing to be trained in the new technology and its use as part of their job role in the patient healthcare process. Therefore, it is not surprising that this study identified organizational culture as one of the sources for EPR information security risks. One of the common risks to information security identified in this study is the risk of the EPR user leaving records open and

going to do something else in another place, forgetting to log out or close the record. This represents poor working practices, an organizational culture issue explored in the interview analysis. This gives an unauthorized person the opportunity to access EPR. The other important risk explored in the organization is passing the EPR information to others, such as relatives, friends, or other stakeholders without the patient's consent or awareness. This is one of the major challenges to the SA NHS, as the EPR is still not considered as a sensitive and critical information document. This is an organizational cultural issue that needs to be solved within the SA NHS.

#### *7.2.3.2 Technology-Based Risks*

The research explored several technology-based risks to information security in SA-NHS. There are also several occasions where users found a problem in accessing and navigating the system and accessed information they did not need. The interview analysis indicated that the current access process does not take into consideration types of information and the staff information needs. The technology is not been used to ensure and enforce information security policy, i.e. to take into consideration staff access to only the information they need.

Unauthorised access to the EPR can be from both external and internal intruders. The externals are usually hackers who are trying to access the system. This access may lead to abuse of the integrity of the EPR information. There is also evidence that internal intruders are accessing EPR without authorization. Internal intruders can lead to abuse of the EPR information. The process used to address such risk is mainly through the ICT department with help and support of the medical records department. The head of each department is also informed of any risk of abuse to any of their departmental employees. This is part of the management process within the hospital. This has been stated in the hospital policy. The ICT department is informed and encouraged to introduce and implement the security policy in their department strictly and firmly to avoid any misuse of the EPR.

A main risk to the EPR can arise from staff using the technology and from the technology itself. The human risk part is based on individual staff behaviour, attitudes and culture. Individual staff may release or pass information to a third party without

awareness of the consequences of such an act. This may be related to the individual culture and organizational culture towards EPR confidentiality. Several interviewees pointed out that several cases had been identified by staff, such as leaving the PC on with EPR information displayed on the monitor without locking the PC or logging out. The other technical problem that may affect information security from the technical point of view is a virus. The virus can create serious problems for the EPR system. The other technical problem is unauthorized access to the EPR system. This is mainly access by hackers. Hackers can be internal or external individuals. Technology is changing rapidly in a very short time. It can be argued that what is secure today may not necessarily be secure tomorrow.

## 7.3 Evaluating EPR

One of the objectives of this study is to evaluate the electronic information security models for health information systems. The EPR model is needed to facilitate the evaluation of the information security policy through establishing an access control policy based on the users, employees, job roles and responsibilities. This study has developed an EPR model based on the following principles:

1. **Type of information:** The patient's care journey in his/her life process is a long journey. The care process from the patient and the medical profession points of view depends largely on the patient record. This large volume of recorded information has a different sensitivity and integrity from the patient's and organisation's point of view. Therefore, it is critically important to classify the electronic patient record information based on its sensitivity and integrity and build information access control based on the need of each of the classifications.
2. **Classification of EPR Users, hospital users:** There are a large number of hospital employees, both medical and non-medical staff. Besides hospital employees, there are external EPR stockholders such as insurance companies, police and national and international regulatory bodies as explained in the SA NHS and the hospital overview in Chapters 1 and 3. Therefore, there is a need to classify the hospital users based on their information needs. Each one of the users needs certain information based on the interest or the role in the patient health care process. From the hospital's point of view, the access should be

based on the employees' need for information only. For this reason, the developed EPR classify and identify the main users of the EPR. Classification of the users with conjunction of the information classification helps to establish and develop information security in the SA-NHS. The developed and designed EPR model took in consideration the EPR users in the design process.

**Information security policy:** One of the key objectives of designing and evaluating is to help in developing and enhancing information security policy in SA NHS (Chapter 1). Information security policy of the EPR is needed to fulfil the SA NHS commitment to have a secure EPR and maintain a professional image in society. The model is designed in such a way as to facilitate the establishment of appropriate information security policy through classification of the information and users' information needs. The information security should be based on need for and use of the information. The principle of information security policy should be based on restricting access to any EPR information apart from the actual needs of the user.

### 7.3.1 Elements of the EPR

One of the main challenges of this study is identifying the main elements in the EPR. This is due to the lack of available EPR designs available in the literature of SA NHS. The research adopted two approaches for identifying these elements of the EPR. The first approach is reviewing and analysing what explored in the literature taking advantage of the work of other researchers in the EPR records. The second approach is collecting data and information using SA NHS. This is needed to ensure the developed EPR model matrix, reflects the SA NHS needs and satisfactions. Merging the main outcomes of the two approaches contributed to the development of the EPR model.

Therefore, one of the main contributions of this research is defining the main elements of the EPR based on type of information. The information types classified based on its nature and sensitivity. This classifications help in designing and implementing access control of the EPR users' based on their role and responsibilities on the patient's care

process. The other contribution of the research is identifying the current situation of EPR security and the policy adopted to secure the information.

The research is arguing towards the needs for a change in the current information security. There is a need to establish a new information security policy to reflect the EPR implementation. There is also a need to change the current EPR access control policy. The access control policy should be based on the user's role and responsibility on the patient's healthcare process. The user should only access the information they need.

## 7.4 EPR Information Security Policy

The focus of this research is the EPR information security policy. Objective 5 stated "*analyse electronic information security policy and methods to verify their consistency*." The main outcomes of the analysis is that the current EPR information security lacks specific policy statements regarding EPR security and the policy is generic and concentrates mainly on access to the EPR. EPR information needs to be protected and secured from any internal and external abuse. The policy needs to be established at several levels of the SA NHS to protect and secure the information. SA is relatively new to information security policy, therefore proposals for a change in the SA NHS current information security is vital to promote and enhance information security.

### 7.4.1 Change in Employees' attitudes and Awareness towards EPR Security

The health service attitudes and awareness towards EPR information security is one of the main elements of protecting EPR information. This study argues strongly in favour of developing employees' attitudes and awareness towards protecting EPR information before establishing information security. Employees are the main actors in handling, transferring, controlling and accessing the EPR. The hospital needs to establish a clear strategy on promoting and enhancing information security for all their employees. This should include the following:

#### *7.4.1.1 Information Security in Induction Day/Week*

There is a need to change the new recruit employee induction day/week. The interview analysis indicated that the current induction does not include the importance and

seriousness of the EPR information security. Importance of information security and its associated policy should be part of the induction plan. The new recruit should be tested in information security to ensure that the information security message is well received and understood by the induction participants.

#### *7.4.1.2 Hospital Employees Training on EPR Information Security*

One of the points raised in the interviews that may contribute to lack of staff awareness towards information security is a lack of training; in fact it does not exist, in EPR security policy. Watanabe et al. (2005; 2011) developed an EPR computer-based self-learning system for students to train them on operations of EPR systems, subjects connected with patient information handling, EPR security and health information ethics. The health services employees are busy due to the high demand of their jobs. However, the hospital authorities need to enforce information security training as part of the employees' Continuous Personal Development (CPD), plan to promote staff awareness towards the importance of complying with the information's security policy and communicating the consequences of not complying with the policy. The training should be compulsory and held annually. This change of approach in staff training contributes positively to EPR information protection and security.

#### *7.4.1.3 Establishing clear SA NHS Information Security Policy*

The Saudi government needs to establish a clear NHS information security policy. This is due to the fact that the SA NHS is centralised as a public service. The SA NHS is sponsored and managed by centralised management, namely the Ministry of Health. The centralised authority helps to enforce the centralised policy. This policy should provide clear information security guidelines.

#### *7.4.1.4 Change the current Hospital Information Security Policy*

The current hospital information security does not meet the expectations and needs of customers, patients, and the national and international legislation. Therefore, there is a need to change the current EPR information security policy. The policy should take into consideration two main factors, types of information of the EPR and types of users. The policy should be established based on access control according to the employees'

job specifications and needs. The employees should be denied access to any information they do not need as part of their job role or to meet their responsibilities in the patient care process.

## 7.5 SA Health Service EPR Policy

This section discusses the SA health services needs for establishing clear policy to protect the EHR.

### 7.5.1 SA National Data Protection Act

The SA authority strategy is to move towards e-government and e-health services. Besides the use of electronic recording, SA citizens have become more aware of their rights regarding their own personal records. The document analysis indicated the lack of a national data protection act to protect individuals rights towards their own data and information. Therefore, the SA needs to establish a data protection act to protect them. The national data protection act can be used to provide guidelines for the organisation to establish their own policy.

### 7.5.2 Policy towards Patient Access

The interview analysis indicated that the medical staff agreed with patients' right to access their EPR and there is no policy for patient access to his/her own EPR. Currently, the hospital needs to establish a clear policy that gives the patient the right to access his/her patient EPR anytime and anywhere. The policy should be clear that the main owner of the EPR is the patient. The other important policy that needs to be formulated is ensuring that medical staff inform patients of their right to access their EPR.

### 7.5.3 Patient's Consent

The document analysis and the interviews indicated that the SA NHS has no policy for patient consent. Therefore, the SA health services need to establish a patient consent policy. The policy needs to state that no individual within the hospital has the right to pass or transfer EPR to a third party without the patient's consent. This is needed as the study found that EPR has been passed to patients' employees without their consent. This has created problems and conflicts.

## 7.6 Summary

The chapter discusses the main outcomes of the research. This includes discussions of the current situation of EPR use in SA and the main risks of implementing EPR in SA. The discussions highlight and explore patients' rights, EPR ownership and the current EPR system used. This chapter also discusses EPR security policy and its implementation into the organisation reality. This includes discussions of the current EPR information security policy and the drives for the change in policy to protect EPR. The discussion stressed the importance of and the need for access control policy.

The main contribution of the research is the development and evaluation of EPR. The model designed to help in developing information security policy and access control strategy. The SA in a position and in a need to change its current information security policy to cope with the information security challenges created by implementing EPR.

# CHAPTER EIGHT:

# CONCLUSIONS, RECOMMENDATIONS AND FURTHER WORK

Objectives

- To provide the research contribution
- To present the study's contributions
- To provide practical recommendations
- To suggest future work based on the study's main outcomes

# 8 CHAPTER 8 : CONCLUSIONS, RECOMMENDATIONS AND FURTHER WORK

## 8.1 Introduction

This chapter summarises the main findings of the thesis and sets the key contributions of this work into the context of the original research problem. As the SA NHS is at the early stage of implementing EPR systems throughout their services, some recommendations based on the findings of this research are presented. The chapter concludes with a critical review of the achievements and will outline a selection of further work in this area arising from this study.

## 8.2 Summary of the Thesis

The qualitative part of this research discovered that a major challenge in the security of healthcare information systems within the SA NHS is the protection of Electronic Patient Records from misuse by internal or external individuals. The responses to the semi-structured interviews have been analysed in Chapter Four and developed the understanding of the current situation of information system security within the SA NHS which formed the basis of this research. Given that EPR security appeared to be the major concern of the respondents interviewed, this study progressed with the analysis of the protections mechanisms of EPR established by security policies and their implementation within a representative hospital, KFH in SA.

A critical analysis of the literature survey was carried out (Chapter Two) to establish the current state of EPR design, its contents and the information security policy needed to protect the security of EPRs. The results of the literature survey were used to augment information that was obtained from the semi-structured interviews to create a model of the EPR as used in the SA-NHS, covering both the stakeholders that use EPR as part of the healthcare processes and the information that is kept within EPRs.

Based on the EPR model, an Electronic Patient Record Matrix (see Chapter Five) has been developed as a tool to compare and analyse access-control properties of EPRs

from both a high-level policy perspective as well as a data-analysis tool for capturing the operational reality of access to EPRs in the KFH .

This model forms part of a wider information security model and has to be seen in this context . The Electronic Patient Record Matrix formed the basis of the second survey that was undertaken as part of this research to identify any discrepancies between the policies in place to protect Electronic Patient Records and the operational reality of their protection. For this purpose, a survey was undertaken in the form of a questionnaire to identify the level of access that various stakeholders in the patient care process have to their EPRs. This information was collated and presented in Chapter Six.

In Chapter Seven the discrepancies between policies and organisational reality as well as conflicting responses between the various stakeholders questioned were analysed and discussed. This served to check for compliance of the day-to-day operations encountered in the hospital with the stated information security policies that are available in the hospital.

## 8.3 Conclusions

The main conclusions of this research can be summarised in the followings:

Identifying and exploring the current situation of EPR

The current situation of EPR security at the NHS can be summarised in the following:

- Lack of recognition and understanding of patient's right.
- The SA NHS has no forms for patient's consent regarding his/her own information that allow transferring and passing his/her EPR to any EPR stakeholders.
- There is no agreement towards who own the EPR, patient or the the hospital management.
- The information security is based on the paper based patient's reord. There is lack of policy regarding EPR.

- Difficult to trace the information security policy, different interpretation of the policy, difficult to access the polic, subjective in dealing with information security issues.

The main risks for implanting EPR include:

- SA NHS organisation culture risks
- Technology based risks

Developing and Evaluating EPR

The research indicated lack of EPR structure and the need to develop model to help in establishing policy. Therefore, the research developed EPR structure model (matrix) based on types of information and EPR users' needs. The main aims of the model is to help and facilitating establishing access control policy.

## 8.4 Contributions

The research has three contributions. Firstly, the qualitative study of the perception of security from the viewpoint of stakeholders in the patient care process has led to the insight that the protection of Electronic Patient Records is considered one of the most important information assets within the SA-NHS. There appeared to be clear problems in the understanding of the security mechanisms involved in the protection of EPRs as well as a lack of security awareness and training from the perspective of staff involved in the handling of EPR. The analysis of the interviews also provided a clear indication that relevant policies are not adequately communicated within the hospital environment, and that they are ambiguous and too imprecise to adequately define the protection requirements of EPRs. This contribution answered the initial research questions "What is the current situation of information system security in SA NHS?" and "What are the main factors influencing Information System Security in SA NHS?". The results are valuable for the SA NHS, as they provide evidence of a lack of security awareness and insufficient management responsibility with respect to information security evidenced

by the lack of detailed policies. The results are also timely as the SA NHS is currently in the process of rolling out EPR throughout its services.

Secondly, the research developed an Electronic Patient Record Matrix for the quantitative analysis of the access control restrictions to information stored on EPR. The matrix has been used both to capture policies and to analyse the operational reality of their implementation. The developed model provides a novel technique for the analysis of access control policies with respect to their consistency and their implementation by populating the model with data obtained from medical personnel involved in the care process. Most contemporary research is based on a purely qualitative foundation and does not provide techniques that allow any objective and quantitative assessment of the conformance to stated security policies with respect to EPRs.

Thirdly, the Electronic Patient Record Matrix as an analysis tool has been evaluated using a quantitative survey of stakeholder access to EPRs. The analysis itself focused predominantly on the effective access rights of stakeholders in the care process as there was insufficient information in any of the available policy documents to perform a more detailed analysis. Nonetheless, the approach has shown that a more objective and quantitative analysis with respect to the protection policies and their implementation is feasible within the healthcare sector and that the developed techniques could be applied to check the conformance with established policies of effective stakeholder permissions during the care process.

## 8.5 Recommendations

The main outcomes of the research stressed the importance of and the need for change throughout the SA NHS to ensure the efficient and effective implementation, use and protection of EPR. The following are the main recommendations to the SA NHS authority that need to be taken into considerations for the introduction, implementation and use of EPR in SA NHS.

### 8.5.1 Developing EPR information security policy throughout the SA NHS

The lack of a clear and consistent policy stresses the need to develop an EPR information security policy throughout the SA NHS. It is highly recommended to develop a national EPR information security policy. This should be led by the SA Ministry of Health and this policy should be reflected throughout the SA NHS such as in the NHS area authority, in hospitals and in departments within the hospitals.

### 8.5.2 Patient's Consent

The current situation in SA NHS ignored and denied the patient's rights with respect to his/her own medical record. The SA NHS needs to introduce and enforce a clear policy on patient consent. Any EPR information should not be accessed or transmitted to a third party such as an insurance company, insurance companies or employer without a written consent from the patient. The SA BHS should design and provide a special form for granting patient consent.

### 8.5.3 Training in EPR information security

One of the main threats to the EPR information security is the SA NHS employees. Therefore, it is highly recommended that the SA NHS authority take into consideration the role of the employees in EPR security. The main tools that can be used to promote and enhance employees' awareness and understanding of EPR information security is regular training. It is highly recommended that all new recruits to the SA NHS need to be inducted in EPR information security policy. It is also recommended that all SA NHS staff attend regular training sessions in EPR security policy at a time, date and location convenient to them. This should be recorded in their training record and the record should be monitored regularly to ensure that employees receive regular training.

### 8.5.4 Access to EPR

Access to EPR authorisation should be controlled by clear policy at the national, SA NHS (Ministry of Health), and hospital levels. Unauthorised access to the EPR must be forbidden throughout the SA NHS services regardless of the position and rank of the user. Unauthorised access must bring about consequences and the consequences for both internal and external users should be clear in the policy.

## 8.6 Future Work

The main outcomes and findings of this study require further research to help in the development of an effective EPR information security policy. The following are the main suggestions for future work:

There is a need for further research in developing a written EPR information security policy for SA NHS based on the main outcomes of this research. The key aspect here is that the results of this study can be used to establish the foundation of a detailed security policy with respect to Electronic Patient Records on the basis of the current reality and requirements for access voiced by health-care stakeholders in both interviews and questionnaires.

There is a need for research into the information security culture focusing on handling EPR among the SA NHS. The research should be focused on SA NHS employees' perception, attitudes and their daily practice with regard to EPR information security.

# REFERENCES

Abdul-gader. (1997). "Information systems strategies for multinational companies in Arab Gulf countries.", *International Journal of Information Management,* 17(1),p.p. 3-12.

Abernethy, A.P; Wheeler, J.L; Bull, J.(2011),"Development of a Health Information Technology–Based Data System in Community-Based Hospice and Palliative Care" American Journal of Preventive Medicine,40(5),p.p. 217-224

Abu-Musa,A. (2010) "Information security governance in Saudi organizations: an empirical study*", Information Management & Computer Security*, 18 (4), p.p.226 – 276

Acharya, Debargh.(2010), "Security in Pervasive Health Care Networks: Current R&D and Future Challenges" Mobile Data Management (MDM), Eleventh International Conference on , vol., no., p.p.305-306, 23-26 May 2010

Adams,T; Budden,M; Hoare,C ;Sanderson,H. (2004), "Lessons from the central Hampshire electronic health record pilot project: issues of data protection and consent" BMJ, 328, N 7444 pp. 871–874

Alhaqbani, B. and Fidge, C. (2008) "Privacy-preserving electronic health record linkage using pseudonym identifiers", *10th International Conference on e-health Networking, Applications and Services (HealthCom)*, p.p.108-117, DOI: 10.1109/HEALTH.2008.4600120URL, Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4600120&isnumber=4600097

Altuwaijri, M. (2008) "Electronic-health in Saudi Arabia", *Saudi Medical Journal*, 29(2), p.p. 171-178

American Health information Management Association (2010) "*What does your personal health record contain?*" Retrieved on July 2010: http://www.myphr.com/what/contents.asp

Anderson, C.L.; Cardell, J.B. (2008),"Reducing the Variability of Wind Power Generation for Participation in Day Ahead Electricity Markets", HICSS,vo1., no.,p.p.178

Anderson, R.J. (1996) "A security policy model for clinical information systems", *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, (6-8), p.p.30-43

Bakker, A. B. (2004) "Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences", *International Journal of Medical Informatics*, 73(3), p.p. 267-270

Ball, E., Chadwick, D.W., Mundy, D. (2003)"Patient privacy in electronic prescription transfer", *Security & Privacy - IEEE*, 1(2), p.p. 77- 80.

Beale, T., Heard, S., and Kalra, D. (2008), "openEHR Architecture: Architecture Overview", *The OpenEHR Foundation*, Available at: http://www.openehr.org/

Becker, M. Y. (2005). " A formal security policy for an NHS electronic health record service" ,Technical Report UCAMCL- TR-628, University of Cambridge Computer Laboratory, March 2005.

Bickford, C. J. and Hunter, K. M. (2006) "*Theories, models, and frameworks*": in Saba, V. and McCormick, K. (Eds.): "*Essentials of nursing informatics*", p.p.89–106, New York: McGraw-Hill

Britto, M ;Wimberg, J. (2009), "Pediatric personal health records: current trends and key challenges", Pediatrics,123 Suppl. 2 ,pp. S97–S99

Carman, D; Britten, N. (1995), "Confidentiality of medical records: the patient's perspective" *Br J Gen Pract*, 45 (398), pp. 485–488

Chang, C., Hwang,H.,Hung,M., Kuang,Kuo., Yen,D. (2009)"Factors affecting cross-hospital exchange of Electronic Medical Records.", Information & Management, 46(2),p.p. 109-115.

Charles, A; Dube, K; Mtenzi, F.(2010) " Electronic Healthcare Information Security" *Advance in information security* ,53,p190.

Clough,P and Nutbrown,C. (2007), "A Students´ Guide to Methodology: Justifying Enquiry", 2nd edition ,London: Sage.

Creswell, J., (2003) "*Research design: Qualitative, Quantitative, and mixed methods approaches*", 2nd ed., Sage Publications: London.

Daniel, S. ; Shinkfield,A. (2007) "Evaluation theory, models, and applications", 1 edition, Jossey-Bass: USA

Dekker, M.A.C., and Etalle, S. (2007) "Audit-Based Access Control for Electronic Health Records", *Electronic Notes in Theoretical Computer Science*, (168), p.p. 221-236

Desroches, C. M., Campbell, E. G., Rao, S. R., Donelan, K., Ferris, T. G., Jha, A., Kaushal,R.,andLevy,D.E.(2008),"Electronic Health Records in Ambulatory Ca re —A National Survey of Physicians", *New England Journal of Medicine*, 359 (1), p.p. 50–60

Drever, E.(2003) "*Using semi-structured interviews in small-scale research A teacher's guide*" Scottish Council for Research in Education , Glasgow.

El Emam, K; Moreau, K ; Jonker, E.(2011), " How Strong are Passwords Used to Protect Personal Health Information in Clinical Trials", J Med Internet Res,13(1)

Feldman, S.S and Horan, T.A. (2011),"Collaboration in electronic medical evidence development: A case study of the Social Security Administration's MEGAHIT System" ,International Journal of Medical Informatics,80(8),p.p 127-140

Ferreira, A., Cruz-correia, R., Antunes, L., and Chadwick, D. (2007) "Access control: how can it improve patients' healthcare?" *Stud Health Techno Inform*, (127), p.p. 65-76

Fink, A. (2003) " the Survey Kit: how to sample in surveys ", 2nd ed., Sage Publications: London.

Geiger, M. and Cranor, L.F. (2006) "Scrubbing stubborn data: An evaluation of counter-forensic privacy tools", *Security & Privacy - IEEE*, 4(5), p.p. 16–25

Gerber, M., and Solms, R. (2008) "Information security requirements - Interpreting the legal aspects", *Computers & Security*, 27(5-6), p.p. 124-135

Gollman D. (1999), "*Computer Security*", John Wiley & Sons

Gordon D,S and Bates,D.W.(2010) "Can Electronic Clinical Documentation Help Prevent Diagnostic Errors?", The New England journal of medicine,362(12),p.p.1066-1069

Gritzalis D., Lambrinoudakis C., (2004), "A Security Architecture for Interconnecting Health Information Systems", *International Journal of Medical Informatics (indexed in ISI/SCI-E)*, 73(3), p.p. 305-309

Haak, M.V.D., Wolff, A.C., Brandner, R., Drings, P., Wannenmacher, M., and Wetter, T. (2003) "Data security and protection in cross-institutional electronic patient records", *Int. J. Med. Inform.*, (70), p.p. 117–130

Harris, S. (2003), "*CISSP All-in-One Exam Guide*", 2nd ed., McGraw-Hill Osborne Media

Haux, R. (2001), "Information processing in healthcare at the start of the third Millennium: potential and limitations", *Methods Inf. Med*, 40(2), p.p.156–162

Hawkey,K ; et al. (2008) "Human, organizational, and technological factors of IT security" In CHI '08 extended abstracts on Human factors in computing systems (CHI EA '08). Florence, Italy, p.p.3639-3644.

Hodg, JG.(2003) " Health information privacy and public Health ", *Journal of Law, Medicine&Ethics,*31(4),p.p.21-22

Hoffman, S., Podgurski, A. (2008), “Finding a cure: the case for regulation and oversight of electronic health record systems”, *Harv J Law Techno*, 22(1), p.p. 1–63

Hone,K; Eloff,J.(2002) “What makes an Effective Information Security Policy”,*Policy Network Security*,20(6),p.p.14-16

House of Commons Health Committee (2007), “*Sixth report of session 2006-07: The Electronic Patient Record*”, London: Her Majesty's Stationery Office.

Househ, M., Al-Tuwaijri, M., Al-Dosari, B. (2010), “Establishing an Electronic Health Centre of Research Excellence (E-CoRE) within the Kingdom of Saudi Arabia”, *Health San Francisco*, 4(1), p.p. 42-46

Huang, L.C., Chu, H.C., Lien, C.Y., Hsiao, C.H. and Kao, T. (2009) “Privacy preservation and information security protection for patients' portable electronic health records”, *Computers in Biology and Medicine*, 39(9), p.p.743-750

Huber,M ; Sunyaev,A ; Krcmar,H.(2008) “Security Analysis of the Health Care Telematics Infrastructure in Germany”, *Proceedings of the 10th International Conference on Enterprise Information Systems*, June 12-16, 2008 (2008), pp. 144-153

Iacovino ,L .” Trus tworthy shared electronic health records: recordkeeping requirements and Health Connect*,” Journal of Law and medicine*,11(1),p.p.40-60

ISO/IEC, (2005) “Information technology – code of practice for information security management, ISO/IEC 27002:2005”, *The International Organization for Standardization/The International Electro-technical Commission.*

Jaeger, P. T. (2007). "Information policy, information access, and democratic participation: The national and international implications of the Bush administrations information politics", *Government Information Quarterly*, 24(4), p.p. 840-859

Jensen, T.B. and Andersen, P.E. (2010), “Can We Rely on Electronic Medical Record Systems to Reduce Medication Errors?”: in *proceedings of the Americas Conference on Information Systems*, Lima, Peru

Jensen, T.B., and Aanestad, M. (2007), “How Healthcare Professionals “Make Sense”of an Electronic Patient Record Adoption”, *Information Systems Management*, 24(1), p.p. 29-42

Jian, W.S ;Wen, H.C ; Scholl, J ; Shabbir, S.A ; Lee,P ; Hsu, C.Y; Li, Y.c. (2011), “The Taiwanese method for providing patients data from multiple hospital EHR systems” Journal of Biomedical Informatics,44(2),p.p. 326-332

Jin, J., Ahn, G.J., Hu, H., Covington, M. and Zhang, X. (2009), “Patient-centric Authorization Framework for Sharing Electronic Health Records”: in *Proceedings of 14th ACM Symposium on Access Control Models And Technologies (SACMAT 2009)*, Stresa, Italy

John, S. Luo, MD (2006), “Electronic Medical Record”, *Primary Psychiatry*, 13(2), p.p. 20-23

Kadam, A. W. (2007). "Information Security Policy Development and Implementation." *Information Systems Securit,y* 16(5),p.p 246-256.

Kahn, S. S. V., (2008) “Medical Record Privacy and Security in a Digital Environment”, *IT Professional*, 10(2), p.p. 46-52

Kannoju, P.R; Sridhar, K. V; Prasad, K. S. R.(2010), "A New Paradigm of Electronic Health Record for Efficient Implementation of Health Care Delivery”, Biomedical Engineering and Sciences, vol., no., p.p.352-354

Katsikas, S.(2000) “Health care management and information systems security: awareness, training or education? ”, *International Journal of Medical* Informatics,60(2),p.p.129-135.

King Faisal Hospital (2010) available from: http://www.kfshrc.edu.sa/wps/portal/En [Accessed 1/4/2010]

Kluge, E.H.W. (2007), “Secure e-Health: Managing risks to patient health data”, *International Journal of Medical Informatics*, 76(5-6), pp. 402-406

Knapp,K ; et al. (2009), “Information security policy: An organizational-level process model”, *Computers & Security*, 28(7), p.p. 493-508

Kotulic, A; Clark, J. (2004) "Why There Aren't More Information Security Research Studies", *Information & Management*, 41(5), p.p.597-607

Littlejohns, P ; Wyatt, J ; Garvican ,L.(2003) “Evaluating computerised health information systems: hard lessons still to be learnt”, *British medical journal (BMJ),*326(7394),p.p.860-863

Lorenzi, N.M., Kouroubali, A., Detmer, D.E., and Bloomrosen, M. (2009), “How to successfully select and implement electronic health records (EHR) in small ambulatory practice settings”, *BMC Medical Informatics and Decision Making*, Available at: www.biomedcentral.com/1472-6947/9/15

Lovis, C., Spahni, S., Cassoni, N. and Geissbuhler, A. (2007) “Comprehensive management of the access to the electronic patient record: Towards trans-institutional networks”, *International Journal of Medical Informatics*, 76(5-6), p.p. 466-470

Lucas,H.(2008) “Information and communications technology for future health systems in developing countries”,*Social Science & Medicine*, 66(10), p.p. 2122-2132

Mandi,K et al. (2009),“Indivo: a personally controlled health record for health information exchange and communication”,BMC Medical Informatics and Decision Making,7 (1) p. 25.

Marchibroda, J. M. (2007) “Health information exchange policy and evaluation” *Journal of Biomedical Informatics*, 40(6), p.p. 11-16.

McBurney, D., and White, T., (2004) “*Research methods*”, Thomson: Australia

Meijden, M.J.V.D., Tange, H.J., Boiten, J., Troost, J. and Hasman, A. (2000) "An experimental electronic patient record for stroke patients", Part 1: Situation analysis, *Int. J. Med. Inform*., 58(59), p.p. 111–125

National Alliance for Health Information Technology (2008), "*Report to the office of the National coordinator Health Information Technology on defining key health information technology terms Department of Health and Human Services*"

National Committee on Vital and Health Statistics (2006), "*Personal health records and personal health record systems: a report and recommendations*", Washington: Department of Health and Human Services, Available at: www.ncvhs.hhs.gov/0602nhiirpt.pdf

Olola, CH; et al. (2011), "The perception of medical professionals and medical students on the usefulness of an emergency medical card and a continuity of care", International Journal of Medical Informatics,80(6),p.p.412-420

P.C. Tang and T.H. Lee. (2009), "Your doctor's office or the internet? Two paths to personal health records" N Engl J Med, 360 (13), p.p. 1276–1278

Pagliari, C., Detmer, D. and Singleton, P. (2007) "Potential of electronic personal health records", *British medical journal (BMJ)*, 335(7615) p.p. 330-333

Patton ,M .(2002), "Qualitative research and evaluation methods", third edition, London :Sage.

Peltier, T.R. (2004), "*Information security policies and procedures: A practitioner's reference*", London, Auerbach Publications

Perera, G ; Holbrook, A ; Thabane, L ; Foster, G Willison, D.J.(2011)," Views on health information sharing and privacy from primary care practices using electronic medical records" ,International Journal of Medical Informatics,80(2),p.p.94-101

Perlin, J.B, Kolodner, R.M. and Rosswell, R.H. (2004), "The veterans health administration: quality value, accountability, and information as transforming strategies for patient-centered care", *Am J Manag Care*, (10), p.p. 828-836

Porter, S ; Kohane,S ; Goldmann,D.(2005). "Parents as Partners in Obtaining the Medication History." ,Journal of the American Medical Informatics Association 12(3),p.p. 299-305.

Predeschly, M., Dadam, P., Acker, H. (2008), "*Security Challenges in Adaptive e-Health Processes*", In SAFECOMP, p.p.181-192

Protti, I. J.D., Perez-Torres, F. (2009), "Comparing the application of Health Information Technology in primary care in Denmark and Andalucía", *International Journal of Medical Informatics*, 78(4), p.p. 270-283

Qurban, M.H., and Austria, R.D. (2008) "Public Perception on E-Health Services: Implications of Preliminary Findings of KFMMC for Military Hospitals in KSA", *European and Mediterranean Conference on Information Systems (EMCIS2008)*

Rice, D., (2008), Geekonomics: The real cost of insecure software. Addison Wesley.

Ross, S.E., and Lin, C.T. (2003), "The effects of promoting patient access to medical records: a review", *J Am Med Inform Assoc*, (10), p.p. 129–38

Sahi (2008), "Saudi E-Health Conference", *Saudi Association for Health Informatics*, Available at: http://www.saudiehealth.org/

Saleh,M; Alrabiah,A;Bakry,S(2007) "Using ISO 17799: 2005 information security management: a STOPE view with six sigma approach", *International Journal of Network Management*,17(1),p.p.85-97.

Sandhu, R; Feinstein, H.L.; Youman, (1996). "Role-based access control models" ,*Computer*, 29(2),p.p. 38-47.

Sekaran, U. and Sekaran, U. (1992). "Research methods for business: a skill building approach", 2nd ed., Wiley: New York, Chichester.

Shoniregun, C.A., Dube, K., and Mtenzi, F. (2010), "Electronic Healthcare Information Security", *Electronic Healthcare Information Security, Advances in Information Security*, (53), ISBN 978-0-387-84817-4, Springer Science Business Media, LLC

Sridhar, G.R., Rao, A.A., Muraleedharan, M.V., Kumar, R.V., and Yarabati, V. (2009), "Electronic medical records and hospital management systems for management of diabetes", *Diabetes and Metabolic Syndrome: Clinical Research and Reviews*, 3(1), p.p. 55-59

Steele, R., and Min, K. (2010), "HealthPass: Fine-Grained Access Control to Portable Personal Health Records", *aina*, *24th IEEE International Conference on Advanced Information Networking and Applications*, p.p.1012-1019

Straub, D. W., Jr. and W. D. Nance.(1990) "Discovering and Disciplining Computer Abuse in Organizations: A Field Study", *MIS Quarterly* 14,45–60.

Sujansky, W.V ; Faus, S.A ; Stone, E ; Brennan, P.F.(2010),"A method to implement fine-grained access control for personal health records through standard relational database queries" Journal of Biomedical Informatics,43(5),p.p.46-50

Van der Linden, H.; Kalra, D.; Hasman, A.; Talmon, J. (2009), "Inter-organizational future proof EHR systems: A review of the security and privacy related issues", *International Journal of Medical Informatics*, 78(3), p.p. 141-160

Wager, K.A., Lee, F.W., and Glaser, J.P. (2009), "*Health Care Information Systems: A Practical Approach for Health Care Management*", Second Edition, Jossey Bass, San-Francisco

Wainer, J., Campos, C.J.R., Salinas, M.D.U., and Sigulem, D. (2008), "Security requirements for a lifelong electronic health record system: an opinion", *Open Med Inform J.*, (2), p.p. 160-165

Watanabe, K.; Yamamoto, K.; Okada, M.; & Takaue, R. (2005), " A computer aided instruction for electronic patient records in a hospital", Japan Journal of Medical Informatics, 25(4), 249-256.

Watanabe,K; Okada,M; Yamamoto,K.(2011),“ EPR (Electronic Patient Record) Laboratory - Simulated Environment to Learn about a Hospital EPR System”, Knowledge Management & E-Learning : an International Journal,3(1),p.p.35-50

Weider, D.Y., Chekhanovskiy, M.A. (2007), “An Electronic Health Record Content Protection System Using SmartCard and PMRTM”, in *Proceedings of the 9th IEEE International Conference on e-Health Networking: Applications and Services (HEALTHCOM 2007)*, 2007, Taipei, Taiwan, p.p. 11-18

Williams,F; Boren,S (2008). "The role of electronic medical record in care delivery in developing countries.",*International Journal of Information Management* 28(6),p.p.503-507.

Yu, W.D. ;Chekhanovskiy, M.A.(2007), “An Electronic Health Record Content Protection System Using SmartCard and PMR” *e-Health Networking, Application and Services, 2007 9th International Conference*,p.p.11-18, 19-22 June 2007

Zhou, Y.Y., Garrido, T., Chin, H.L., Wiesenthal, A.M., and Liang, L.L.(2007), “Patient access to an electronic health record with secure messaging : Impact on primary care utilization”, *The American journal of managed care*, 13(7), p.p. 418-424.

# Appendix A: Interviews

## DE MONTFORT UNIVERSTY

## Information System Security in Health Service

**In-depth Semi-structured interview**

Mouhamad Aldajani

Q1. Does your organization store and process patient records electronically?

.....

Q2.Do you have access to these electronic records?

.....

Q3.What are the information elements of the EPR you use?

.....

Q4.Are there any items you think should not be stored in an EPR. Could you please give your reason for this?

.....

Q5.Are there any items you think should be stored in an EPR that are currently not present. Could you please give your reasons for this?

.....

Q6.Do you have sufficient access rights to a patient's EPR to do carry out your job?

.....

Q7.If you do not have sufficient rights, what parts of the record would you need access to and why?

.....

Q8.Are there any parts of the record that you have access to that you feel are not necessary for you to carry out your job?

.....

Q9.Which items of patient medical record you perceive as being confidential and which not?

.....

Q10.Who do you think is the owner of an EPR?

.....

Q11.Who do you think is the owner of information you write into an EPR?

.....

Q12.Would you allow a patient to read what you are entering in his/her EPR over the course of a treatment?

.....

Q13.Do you allow patients to access to his/ her EPR? (are there any restrictions you are aware of)

.....

Q14. How do you access an EPR?

.....

Q15.Can an EPR be accessed in any other way?

.....

Q16.What information can you access in an EPR (are there any restrictions to this access?)

.....

Q17.Are there any restrictions to this access (e.g. the patient must give his consent or dependence on the patients medical condition)

.....

Q18.Can you pass your access rights to someone else (if yes, are there any restrictions)

.....

Q19.Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)

.....

Q20.Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)

.....

Q21.Can you comment on entries in an EPR?
.....

Q22.Is your access to the EPR logged and audited?
.....

Q23.Have you been trained on the information security aspects of your EPR system?
.....

Q24.Have you been given a security policy document for EPR system?
.....

Q25.Who is responsible for this policy, whom would you ask for clarification if you are unsure?
.....

Q26.If access is controlled as part of the system you are using, who is determining the access rights?
.....

Q27.Are you aware of any security risks arising from the use of EPR?
.....

Q28.Are you/ your organization actively addressing any of these risks? If yes, how?
.....

Q29.Have you experienced any situations where you feel a patient's privacy was at risk? Can you identify
the part of the EPR system that failed to protect the patient?
.....

# Appendix B: Questionnaire

**Dear Participants,**

I am currently pursuing PhD research at De Montfort University, United Kingdom. A key aim of my research is to explore, investigate and analyse information systems security, with a particular focus on Saudi health services. Key research objectives include investigation of the current situation regarding information systems in health services in Saudi Arabia, analysis of information security policy and methods to verify their consistency, identification of the main problems and barriers for the information system security system with respect to organisation reality and investigation of the impact of organisation culture on the information systems security.

I would like your kind contribution in the research process by completing the attached questionnaire. The data derived from the questionnaires will be used in analysing and recommendations for high level security of electronic patient records used at your workplace.

I would also like to stress that all responses will be treated confidentially and will be anonymised. Please do not hesitate to contact me if you needs any clarification or question.

Mohammad Aldajani
De Montfort University,
Leicester, UK.
Email: aldajani@dmu.ac.uk

**Q1:** Please specify which discipline matches your job-role closest (select only one answer)

| Hospital Staff | | |
|---|---|---|
| 1 | Consultant | ☐ |
| 2 | Registrar | ☐ |
| 3 | Resident | ☐ |
| 4 | Anesthetist | ☐ |
| 5 | Medical Student | ☐ |
| 6 | Nurse | ☐ |
| 7 | Matron | ☐ |
| 8 | Pharmacist | ☐ |
| 9 | Medical lab Technician | ☐ |
| 10 | Radiologist | ☐ |
| 11 | Research/Development Coordinator | ☐ |
| 12 | Senior Manager | ☐ |
| 13 | Head of Department | ☐ |
| 14 | MIS Members | ☐ |
| 15 | NHS Regulatory (Audit) | ☐ |
| 16 | Administrator | ☐ |
| 17 | Receptionist | ☐ |
| 18 | Other (Specify the discipline) …….. | ☐ |

**Q2**: As part of the job-role you have given in Q1 do you have access to information that you need.

[]YES

[ ] NO

If YES, please specify the information you need to access and whether you need read, update rights. Please, use the following keys in your response

**READ** : You can READ the contents of the section
**Update** : You can update the record by adding new information and save the record
**Not needed** : Not part of your job role and responsibilities

☐ √

Please tick √ the appropriate box based,

Patient Identity Information

| | | Read | Update | Not needed |
|---|---|---|---|---|
| **1** | Patient Hospital Code | ☐ | ☐ | ☐ |
| **2** | Patient title | ☐ | ☐ | ☐ |
| **3** | Patient surname | ☐ | ☐ | ☐ |
| **4** | Patient first name | ☐ | ☐ | ☐ |
| **5** | Patient Photograph | ☐ | ☐ | ☐ |
| **6** | Patient Mother Name | ☐ | ☐ | ☐ |
| **7** | Date of birth | ☐ | ☐ | ☐ |
| **8** | Other, Please specify:……. | ☐ | ☐ | ☐ |

**Q3**: As part of your job do you have access to Patient personal Information?

[ ] YES

[ ] NO

If YES, please specify the information you have to access and whether you need read, update rights.

Patient personal Information

| | | Read | Update | Not needed |
|---|---|---|---|---|
| **1** | Marital Status | ☐ | ☐ | ☐ |
| **2** | Home Tel Number | ☐ | ☐ | ☐ |
| **3** | Mobile Number | ☐ | ☐ | ☐ |
| **4** | Gender | ☐ | ☐ | ☐ |
| **5** | Home Address | ☐ | ☐ | ☐ |
| **6** | Religious | ☐ | ☐ | ☐ |
| **7** | Ethnic background | ☐ | ☐ | ☐ |
| **8** | Nationality | ☐ | ☐ | ☐ |
| **9** | Date of Death | ☐ | ☐ | ☐ |
| **10** | Other, please specifiy:……. | ☐ | ☐ | ☐ |

**Q4** : As part of your job do you have access to Patient Personal Related Record?

[]YES

[ ] NO

If YES, please specify the information you have to access, to accomplish your job, and whether you need read, update rights.

Patient Personal Related Record

| | | Read | Update | Not needed |
|---|---|---|---|---|
| **1** | First Full kin Name | ☐ | ☐ | ☐ |
| **2** | First kin Address | ☐ | ☐ | ☐ |
| **3** | First kin Tel No | ☐ | ☐ | ☐ |
| **4** | GP Name | ☐ | ☐ | ☐ |
| **5** | Surgery Name | ☐ | ☐ | ☐ |
| **6** | Surgery Address | ☐ | ☐ | ☐ |
| **7** | Surgery Tel No | ☐ | ☐ | ☐ |
| **8** | Workplace Name | ☐ | ☐ | ☐ |
| **9** | Workplace address | ☐ | ☐ | ☐ |
| **10** | Workplace Tel No | ☐ | ☐ | ☐ |
| **11** | Donor Status | ☐ | ☐ | ☐ |
| **12** | Other, please specify:…… | ☐ | ☐ | ☐ |

**Q5**: As part of your job do you have access to Patient Appointment Record?

[]YES

[ ] NO

If YES, please specify the information you have to access, to accomplish your job, and whether you need read, update rights.

Patient Appointment Record

| | | Read | Update | Not needed |
|---|---|---|---|---|
| **1** | Hospital Department Code | ☐ | ☐ | ☐ |
| **2** | Hospital Department Patient No | ☐ | ☐ | ☐ |
| **3** | Hospital Department Name | ☐ | ☐ | ☐ |
| **4** | Time of Appointment | ☐ | ☐ | ☐ |
| **5** | Date of Appointment | ☐ | ☐ | ☐ |
| **6** | Discharge Time | ☐ | ☐ | ☐ |
| **7** | Discharge Date | ☐ | ☐ | ☐ |
| **8** | Cancellation Time and Rebooking | ☐ | ☐ | ☐ |
| **9** | Cancellation Date and Rebooking | ☐ | ☐ | ☐ |
| **10** | Hospital Department Consultant | ☐ | ☐ | ☐ |
| **11** | Hospital Department Senior Nurse | ☐ | ☐ | ☐ |
| **12** | Referred from | ☐ | ☐ | ☐ |
| **13** | Referred to | ☐ | ☐ | ☐ |
| **14** | Comments | ☐ | ☐ | ☐ |
| **15** | Updated By and Date (Staff Name) | ☐ | ☐ | ☐ |
| **16** | Other, please specify:…… | ☐ | ☐ | ☐ |

**Q6**: As part of your job do you have access to Non-Clinical Information?

[]YES

[ ] NO

If YES, please specify the information you have to access to accomplish your job and whether you need read, update rights.

Non-Clinical Information

| | | Read | Update | Not needed |
|---|---|---|---|---|
| **1** | Hospital Name | ☐ | ☐ | ☐ |
| **2** | Hospital Address | ☐ | ☐ | ☐ |
| **3** | Hospital Telephone Number. | ☐ | ☐ | ☐ |
| **4** | Ward Number | ☐ | ☐ | ☐ |
| **5** | Room Number | ☐ | ☐ | ☐ |

| | | | | |
|---|---|---|---|---|
| **6** | Bed Number | ☐ | ☐ | ☐ |
| **7** | Consultant in patient care Charge Name | ☐ | ☐ | ☐ |
| **8** | Physician/Resident in Charge Name | ☐ | ☐ | ☐ |
| **9** | Senior Nurse in Charge Name | ☐ | ☐ | ☐ |
| **10** | Nurse in patient care Charge Name | ☐ | ☐ | ☐ |
| **11** | Other, Please specify:…….. | ☐ | ☐ | ☐ |

**Q7** :As part of your job do you have access to Patient Medical History?

[]YES

[ ] NO

If YES, please specify the information you have to access, to accomplish your job ,and whether you need read, update rights.

Patient Medical History and Examination

| | | **Read** | **Update** | **Not needed** |
|---|---|---|---|---|
| **1** | Patient allergies | ☐ | ☐ | ☐ |
| **2** | Previous diagnose illness | ☐ | ☐ | ☐ |
| **3** | Patient Smoking | ☐ | ☐ | ☐ |
| **4** | Patient Alcohol Drinking | ☐ | ☐ | ☐ |
| **5** | Clinical test | ☐ | ☐ | ☐ |
| **6** | Surgical Operations | ☐ | ☐ | ☐ |
| **7** | Surgical Operations | ☐ | ☐ | ☐ |
| **8** | Family medical history | ☐ | ☐ | ☐ |
| **9** | Other, please specify:……. | ☐ | ☐ | ☐ |

**Q8**: As part of your job do you have access to Patient Medication?

[]YES

[ ] NO

If YES, please specify the information you have to access, to accomplish your job, and whether you need read, update rights.

Patient Medication

| | | Read | Update | Not needed |
|---|---|---|---|---|
| **1** | Medicine Name | ☐ | ☐ | ☐ |
| **2** | Medicine Taken Date | ☐ | ☐ | ☐ |
| **3** | Medicine Dose | ☐ | ☐ | ☐ |
| **4** | Medicine Type/route | ☐ | ☐ | ☐ |
| **5** | Other, please specify:…….. | ☐ | ☐ | ☐ |

**Q9** As part of your job do you have access to Investigation?

[]YES

[ ] NO

If YES, please specify the information you have to access, to accomplish your job, and whether you need read, update rights.

Investigations

| | | Read | Update | Not needed |
|---|---|---|---|---|
| **1** | Blood test | ☐ | ☐ | ☐ |
| **2** | Urine test | ☐ | ☐ | ☐ |
| **3** | Stool test | ☐ | ☐ | ☐ |
| **4** | other Laboratory tests | ☐ | ☐ | ☐ |
| 5 | X-ray and other Radiological tests | ☐ | ☐ | ☐ |
| 6 | Other tests, Please specify:……. | ☐ | ☐ | ☐ |

**Q10:** Please write any comments you wish to make regarding the EPR?

**Many Thanks for your time.**

1. Once you have completed the questionnaire, can I ask you kindly to return the questionnaire with the provided self-addressed envelope to the hospital main reception in person or through the hospital internal mailing system.

2. If you have any queries or questions regarding the questionnaire please
    a. Leave a message to the researcher with the hospital main reception.
    b. E-mail the researcher: aldajani@dmu.ac.uk

# Appendix C: Interview Transcript

**Interview No 1**

**Manager 1**

**Q1: Does your organization store and process patient records electronically?**

*Part of his majesty vision and plan is to improve healthcare services to the Saudi society. His majesty government has a strategy toward e-health care and services. Our hospital has been selected to be one of the hospitals by Ministry of Health to introduce and implements EPR systems. EPR has helped a lot of issues from the management point of view such as the insurance issue of non-Saudi. There is a large number of non-Saudi in the Saudi labour market. They have different insurance types and coming from different countries. There is a need to identify the patient nationality to help in identifying the insurance policy and identifying the country in case of death. It is also important to stress identifying nationality of patients helps identifying patient background, previous nutrients, medical history and in statistical analysis of NHS plan and performance*"

**Q2: Do you have access to these electronic records?**

*Yes, I have access to the record as I needed to check some management issue regarding the patient healthcare management.*

**Q3: What are the information elements of the EPR you use?**

*Generally speaking, I do not use the information element of the EPR. However, in case of cooperation with policy, insurance company or with the patient for various reasons I need to use some information of the EPR such as his personal details, length of stay, and his/her illness as example.*

**Q4: Are there any items you think should not be stored in an EPR. Could you please give your reason for this?**

*The current items of the EPR based on my use and understanding is what we need and there is no information that we do not to use. From managerial position, I have not received a request or comments to remove or the information of the EPR should not be stored.*

**Q5: Are there any items you think should be stored in an EPR that are currently not present. Could you please give your reasons for this?**

*From the management point of view, the EPR system should also include cost of the patient care in the process. I also like to state hours and time spent by the doctors in the care process.*

**Q6: Do you have sufficient access rights to a patient's EPR to do carry out your job?**

*Yes and do not forget I do not need details of the patient medical conditions. In our daily work, we have several communications with the Health Ministry and with other hospitals regarding patients in our patient in several occasions that enquire is not sure which hospital is the patient. A database with hospital code in the EPR helps to facilitate communications with various patients' stockholders and facilitating patient health care. One of the main challenges in patient's management in SA NHS management is*

*patients care management, monitoring patient's health care and appropriate plan for the NHS. I personally strongly believe there is a need for NHS number for each SA citizens"*.

**Q7: If you do not have sufficient rights, what parts of the record would you need access to and why?**

Not applicable

**Q8: Are there any parts of the record that you have access to that you feel are not necessary for you to carry out your job?**

*The patient medical history and medicine taken and so on I do not them. They are not part of my job or responsibility.*

**Q9: Which items of patient medical record you perceive as being confidential and which not?**

*I think the patient personal details is not confidential but the medical information is confidential information. As hospital we should ensure the security of the information and we do our best to keep the record safe.*

**Q10: Who do you think is the owner of an EPR**

*We are the hospital, NHS, are the owner of the EPR. The EPR created by our professional staff, stored and maintained by our organization. The only body who has right to pass store and transfer the record is the organization itself.*

**Q11: Who do you think is the owner of information you write into an EPR**

*I do not write into the EPR is not part of my job role and responsibility.*

**Q12 would you allow a patient to read what you are entering in his/her EPR over the course of a treatment?**

*I am not member of medical staff, the question should be directed to our medical staff.*

**Q13 Do you allow patients to access to his/ her EPR? (are there any restrictions you are aware of)**

*The patient has enough information to their medical record through their medical doctor. They provide the patient regarding their medical conditions and the medicines need to be take. Personally, is not part of my job to allow the patient access to hi or her EPR record*

**Q14: How do you access an EPR?**

*Using username and password as any access process for any system. We have robust system to control the use of the username and password,*

**Q15: Can an EPR be accessed in any other way?**

*No, it is not possible as our system very strong and reliable. We have a well trained ICT team working hard to ensure security of the EPR. We also buy latest technology to ensure no intruder enter our system.*

**Q16: What information can you access in an EPR (are there any restrictions to this access?**

*As I said before, I have access I need the general information related to the the patient. I need them from managing the patient case point of view.*

**Q17: Are there any restrictions to this access (e.g. the patient must give his consent or dependence on the patient's medical condition)**

*There is no need to take patient consent for accessing EPR. The data and information created by the hospital and the EPR ownership must be kept within the hospital.*

**Q18: Can you pass your access rights to someone else (if yes, are there any restrictions)**

*No, I cannot. This is against out policy and practice. No one should pass his access right to somebody else. There is a heavy consequence if we found such a case.*

**Q19: Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)**

*No I cannot, the system does not allow to do any changes to the EPR. It is not part of my job. However, nobody should do it.*

**Q20: Can you modify/change/delete entries others have made to an EPR (if yes, are there any restrictions)**

*No I cannot, this is against the principle and policy of the hospital, nobody should have the power to modify somebody else entries.*

**Q21: Can you comment on entries in an EPR?**

The EPR entries are excellent and reflect the hospital needs and satisfactions. The only I think I need some of the non-medical entries to be added such calculating the cost and time spent to help us as management to run our hospital with high efficiency.

**Q22: Is your access to the EPR logged and audited?**

*ICT team is logging the systems regularly to trace the changes and who carried out the changes. From, the auditing point of view, we carry out auditing from time to time. At the current EPR system we have not done any auditing as the system is relatively new.*

**Q23: Have you been trained on the information security aspects of your EPR system?**

*Yes, I had brief training one the system by one of our ICT team. It was on-to-one training. The training helped me to understand the system and how to use the system to carry out my job.*

**Q24: Have you been given a security policy document for you EPR system?**

*EPR is one of the important confidential documents in the hospital. We have clear policy to ensure its confidentiality of the records. We have robust iCT policy and each member of staff should have his or her won password and username to access our system. We are very serious for any abuse to our system*. Our policy clear. We may not

have specific EPR policy but the ICT policy mat be enough at this stage.

**Q25: Who is responsible for this policy, whom would you ask for clarification if you are unsure?**

*We are public services organization working under the Ministry of Health. We are one of their hospitals. The ministry of Health has a responsibility towards establishing the national information health policy and its security. This needs to be part of his Majesty government. The hospital itself I meant the senior management of the hospital has a responsibility of translating the Ministry of Health policy and strategy. The hospital needs to develop a policy reflecting its EPR activities and operations.*

**Q26: If access is controlled as part of the system you are using, who is determining the access rights?**

*We are as hospital management control the access right in principle. WE decide the access control to the system. ICT department is our tool for implementing our decision as they are technically equipped to implement the access control policy.*

**Q27: Are you aware of any security risks arising from the use of EPR.**

*I am not aware of any risks arise from the use of EPR. I have not heard and have not seen any report suggesting risks from using EPR. The system as I understand and aware is secured and there is no any risks associated with its use.*

**Q28: Are you/ your organization actively addressing any of these risks? If yes, how?**

*Part of our management style is addressing any any risk from any sources. As you are aware, Our services is sensitive and play a major role on the government and society image. Therefore, we are very serious in addressing any risk to our EPR system. However, we have not received any complain so far.*

**Q29: Have you experienced any situations were you feel a patient's privacy was at risk? Can you identify the part of the EPR system that failed to protect the patient?**

*No, I have not experienced any situations where the patient's privacy was at risk. Not al all.*

## Interview No 2

## Physician 1

**Q1: Does your organization store and process patient records electronically?**

*My reply to your question is yes we do use EPR in the hospital. The hospital bought a good system to achieve introducing electronic recording. In fact currently* "most of our patient medical record carried out electronically. It is quiet useful and saving a lot of time and effort.

**Q2: Do you have access to these electronic records?**

*From my first day in the hospital I have given me access to EPR. I have no restriction in accessing EPR. In fact I am using the access to EPR as part of my job responsibilities in the hospital. I believe and understand that all the hospital physicians have access to the EPR.*

**Q3: What are the information elements of the EPR you use?**

*Well, as you now as a physician, I need any information related to the patient. Patient information is critical for the patient care process. The data bases should be designed and directed to facilitate the physicians need.*

**Q4: Are there any items you think should not be stored in an EPR. Could you please give your reason for this?**

*I strongly believe in principle any items that not serve the patient health are process should not be included in the EPR. At present there is no item I can identify as not related.*

**Q5: Are there any items you think should be stored in an EPR that are currently not present. Could you please give your reasons for this?**

*There is a need to collect medical information as much as we can before preceding the medical process in the hospital. There is a need to interact with previous patient medical providers for consultation and getting more information when it is required. Therefore, strongly believe the EPR needs to stated the local doctor name, the local surgery name, address and telephone number.*

**Q6: Do you have sufficient access rights to a patient's EPR to do carry out your job?**

*In fact as I explained earlier I have full access to EPR and I have no problem in accessing EPR. From the first day of my employment in the hospital I have given full permission to access EPR.*

**Q7: If you do not have sufficient rights, what parts of the record would you need**

**access to and why?**

Not applicable

**Q8: Are there any parts of the record that you have access to that you feel are not necessary for you to carry out your job?**

*No, as a physician I need as much information about my patient as possible. This includes even his social or financial. These may have impact on the patient health. This is why; I highly believe physicians need to be in the system evaluation process.*

**Q9: Which items of patient medical record you perceive as being confidential and which not?**

*Listen, … I strongly believe that the patient is the owner of the information. Therefore, all the information regardless of its sensitivity is confidential and should not be public without appropriate consent from the hospital. At the moment the hospital has no patient consent process or forms*!! Why the hospital does not have process or consent? *I do not know you may need to ask the hospital authority.*

**Q10: Who do you think is the owner of an EPR**

*As I said earlier, the patient is the owner of the EPR. I do believe the hospital and the staff contribute in generating the EPR and paying for the system but the nature of the information is still personal and should be owned by the patient.*

**Q11: Who do you think is the owner of information you write into an EPR**

*The information I write in the EPR represents my personal professional judgment in the patient case. However, the information is based on the patient personal information therefore the professional judgment in the case stay as patient personal information. Do nor forget, I am paid to make decision in the patient cases.*

**Q12 would you allow a patient to read what you are entering in his/her EPR over the course of a treatment?**

*The patient has full right to their medical record and I am strongly to establish a process for the patient to access their medical record. In fact, it is part of the medical care process to inform the patient about his medical condition, medicine and allergies.*

**Q13 Do you allow patients to access to his/ her EPR? (are there any restrictions you are aware of)**

*Yes, I always give the patient full access to his own information at the patient convenient time. I have no any restriction to any information. As I told you earlier, the patient is sole owner of the EPR.*

**Q14: How do you access an EPR?**

*The hospital ICT department established User name and Password for accessing the EPR. I have my own user name and I have set my own password. Using them enables me accessing the EPR at any terminal available in the hospital.*

**Q15: Can an EPR be accessed in any other way?**

*Well, I am not expert in ICT, BUT I believe there is no any other way for accessing the EPR other than using the user name and the password provided by ICT department.*

**Q16: What information can you access in an EPR (are there any restrictions to this access?**

*As explained earlier, I have full access to my patients; EPR. There is no any restriction to my access. I believe this is the case for all hospital physicians. Any how,, as I explained to you before, physicians need full information regarding their patients. Possibly, I may have restriction accessing other patients in other hospital or department in which I do not need to access such information anyhow.*

**Q17: Are there any restrictions to this access (e.g. the patient must give his consent or dependence on the patient's medical condition)**

*There is no any restriction to my access and as far I know there is no or I have not seen patient consent for accessing his/her own EPR. I think, this may need to be addressed as part of the patient right. May be the hospital needs to establish a process for the patient consent.*

**Q18: Can you pass your access rights to someone else (if yes, are there any restrictions)**

*No, I have no right to pass my own right access to someone else. It is against the hospital rules, regulations as well as against my personal principles. The EPR access privilege remains personal*

*and should not pass to anybody internally or externally. In simple language I have no right to pass my access right to somebody else and ethically is wrong.*

**Q19: Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)**

*Yes, I can add new information, you know and understand, part of my job, is entering the new information to the EPR. I need to update the information based on the new medical tests and diagnosis. I need to stress, I can not modify, change or delete previous, already exists information, on the EPR. The system does not allow us.*

**Q20: Can you modify/change/delete entries others have made to an EPR (if yes, are there any restrictions)**

*Not part of our profession to change previous patient medical record. It is bad practice and unprofessional. We usually use previous information to help us in making decision in the patient case as previous information is important in the patient decision. However, the current system does not allow us to modify, change or delete already exist information.*

**Q21: Can you comment on entries in an EPR?**

The EPR entries are reasonable and meet the basic principle needs of the physicians. However, I believe the entries need to be modified and updated as the patient health care process and patient right are changing and the EPR needs to cope with such changes.

**Q22: Is your access to the EPR logged and audited?**

*Usually the physician not involves in quality assurance policies and actions due to the nature of the physicians jobs and they do not have time to involve in such processes.*

**Q23: Have you been trained on the information security aspects of your EPR system?**

*Yes, I have been in training in the United Stated part of the hospital team visited the States for the training purposes. The training was part of the contract between the hospital and the system provider.*

**Q24: Have you been given a security policy document for you EPR system?**

*The hospital has certain rules and procedures for security policy. I have been given the document but I believe the document needs improvement and updating. There is no clear reliability and security related issues.* **Sorry, What do you mean? Can you explain**. *There is lack of statement ensuring the reliability of the system we are using and security. There is a need for guarantee statement from the American supplier of the system and from the hospital ICT department. This is needed to motivate the medical staff and patients to use the EPR system.*

**Q25: Who is responsible for this policy, whom would you ask for clarification if you are unsure?**

*Senior management, the hospital authority, is responsible for the hospital policies and strategy. One of these responsibilities is the policy towards EPR security.* ***What's about if you are unsure****? I usually ask my senior staff for clarification or one of the medical staff such as the senior nurse.*

**Q26: If access is controlled as part of the system you are using, who is determining the access rights?**

*My access is mainly controlled by senior management based on my job rules. Medical record department particularly is the one who set my access rights.*

**Q27: Are you aware of any security risks arising from the use of EPR.**

*The main risk is the possibility of breaching patient privacy. Traditional patient medical record is difficult to cope, transfer, copy and edit. In other hand, the EPR is opposite. Therefore, I stress the main risk of using EPR is the possibility of breaching patient personal and medical information. From personal experience based my observation, the main risks arising from use of EPR, I have seen staff forget to log off from their machine after their entries and leaving the EPR opened. This may be opportunity for intruder to access EPR and abuse the system.*

**Q28: Are you/ your organization actively addressing any of these risks? If yes, how?**

*Medical record department is addressing any security issues and deal with it accordingly. However, there is no clear policy and or strategy on security policy. I feel the hospital needs a well structured system in addressing risks. At the moment, I feel still not under control. I feel, there is a need bringing, the hospital management, EPR users and ICT department to discuss and establish process for addressing risks issues, I am just suggesting!*

**Q29: Have you experienced any situations were you feel a patient's privacy was at risk? Can you identify the part of the EPR system that failed to protect the patient?**

*As I explained earlier, the main experience I got regarding the patient privacy' is mainly due to misuse of the EPR. Some time, member of medical staff leave their PC logged on with EPR open and leaving their desk. I feel, this expose the patient privacy at risk. The other situation I experienced is the access control needs to be more restricted.* **For example**, *I have seen nurse with full access to EPR. I believe each staff should only allowed to access what he needs based on his/her job role and responsibilities.*

## Interview No 3
## Physician 2

**Q1: Does your organization store and process patient records electronically?**

*Our hospital is one of the first hospitals in the Kingdom introduced and implemented EPR system to facilitate our operations and help to meet the national authority expectation and vision in improving healthcare to the SA citizens using.*

**Q2: Do you have access to these electronic records?**

*Yes of course otherwise how I am going to carry out my daily job which is mainly providing healthcare to patient. I have given full access to the hospital electronic record at my first day in the job in the hospital. This is good from the hospital management point of view.*

**Q3: What are the information elements of the EPR you use?**

*I mainly needs the patients full personal details to ensure I am dealing with the right patient. Especially in Saudi Arabia we large number of patient's sharing the same surname, tribe name as you*

*know. I also needs in details the patient's medical history and his/her current medical problems.*

**Q4: Are there any items you think should not be stored in an EPR. Could you please give your reason for this?**

*No, I cannot see any items currently in the system need to be deleted. This is simple patient's information is critical for his/her medical decisions. I have not seen any information that is not needed.*

**Q5: Are there any items you think should be stored in an EPR that are currently not present. Could you please give your reasons for this?**

*The digital video technology need to be used as part of the EPR. Patient's previous operations and diagnosing case can be recorded by digital media. These extra can be used to help the medical staff in decision making. The technology is there now and should be used in the health services recording processes.*

**Q6: Do you have sufficient access rights to a patient's EPR to do carry out your job?**

*Yes, no problem with my access right. From day one I have given the username and password with full access to the EPR system. AS a physician in the hospital, It is important and critical to have full access in order to carry out my job properly.*

**Q7: If you do not have sufficient rights, what parts of the record would you need access to and why?**

Not applicable

**Q8: Are there any parts of the record that you have access to that you feel are**

**not necessary for you to carry out your job?**

*The current EPR system has no item related to patient that I feel that they are not necessary or needed in the systems. The current items well selected and throughout about. Possibly we need more information to be added to the EPR system.*

**Q9: Which items of patient medical record you perceive as being confidential and which not?**

*The whole document for me and for the hospital is confidential record. The record has personal information created and managed by the hospital and its contents purely concerning one individual human. The individual personal details should be respected by everybody and should be respected by the hospital. The hospital should all effort to keep the EPR private and confidential. We can not say this part is confidential and this part is not.*

**Q10: Who do you think is the owner of an EPR**

*The owner of the EPR is the patient. The patient should have the access and carry out his record wherever he likes during his healthcare process. In my view, the patient should have a copy of his record with him after any visit to the hospital.*

**Q11: Who do you think is the owner of information you write into an EPR**

*The owner of what I write should be the patient. My writing is my professional judgment and decision towards the patient case. So, it doesn't matter who write in the EPR, the owner remain the hospital. We have been paid to write into the EPR. It is part of our job and responsibilities toward the patient's healthcare process.*

**Q12 would you allow a patient to read what you are entering in his/her EPR over the course of a treatment?**

*Yes, no problem and part of my job I read what I write on the EPR and I always make sure the patient's understand what I read to him and happy for the patient o read what I have written on my monitor.*

**Q13 Do you allow patients to access to his/ her EPR? (are there any restrictions you are aware of)**

*Yes, I always give the patient full access to his/her information at the patient convenient time. I have no any restriction to any information. As I told you earlier, the patient is sole owner of the EPR.*

**Q14: How do you access an EPR?**

*Just by using my personal username and password. Theses have been set by the ICT department. I have the chance to change my password in which I do from time to time to ensure nobody can use my personal access right.*

**Q15: Can an EPR be accessed in any other way?**

*No, it is not possible. The technology does not allow it. There are hackers but they are illegal and I have not experienced one in our hospital.*

**Q16: What information can you access in an EPR (are there any restrictions to**

**this access?**

*I have access to the EPR without any specific restriction. This access right is needed to carry out my duty with towards the patient. You understand the physician needs every single of data and information regarding the patient in order to make the appropriate decision towards the patient case. The decision is the most important and critical in patient healthcare process*

**Q17: Are there any restrictions to this access (e.g. the patient must give his consent or dependence on the patient's medical condition)**

*No, there is no any restriction to the access. Currently there is no any process or forms for patient consent. The patient's record transferred to different stakeholders without patient consent. This is not right in my view*

**Q18: Can you pass your access rights to someone else (if yes, are there any restrictions)**

*Patient medical condition, diagnosis, critical needs to be kept confidential and should not be accessed by anyone apart from the patient medical physician without the patient consent*.

**Q19: Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)**

*Yes I can modify, change and delete during the writing process of the entry. IF I wrote something and I am still in the writing cell and before saving the record I can change and modify but once I save the entry I have no right to change or modify the entry.*

**Q20: Can you modify/change/delete entries others have made to an EPR (if yes, are there any restrictions)**

*No, not at all, the system does not allow it. I can read my colleagues writing but I can not change their entry.*

**Q21: Can you comment on entries in an EPR?**

*The patient electronic records are still in the process of development. There are several items need to be added to the electronic record such as the clinical testing. The hospital is still using paper based recording system.* The current EPR design needs to be changed to make it more easy to use and clearer. I found it difficult to navigate and search for information for patient with long medical history*"*. (Interview 3, Physician)

**Q22: Is your access to the EPR logged and audited?**

*As far as I am aware I have not seen any auditing or aware of EPR logging system. It could be done without my knowledge, to be honest I do not know,*

**Q23: Have you been trained on the information security aspects of your EPR system?**

*Yes, I have internal training in my department. It was one-to-one training. In the training, they showed me the system functionality, capability and how to use the system.*

**Q24: Have you been given a security policy document for you EPR system?**

*If your interview mainly to discuss EPR policy within our hospital, the first issue we need to discuss the EPR policy. I do like to stress the first step in adopting EPR system in the hospital is to establish EPR policy without it we cannot move forward regarding the EPR security, and nobody gave us one. …. Clear policy helps us in identifying our roles and responsibilities toward EPR. There is no clear statement regarding the EPR security. The current policy is generic ICT policy. There is a need for clear policy regarding use of EPR. Policy copied from other hospital policy without taking in consideration the cultural and the hospital current activity*

**Q25: Who is responsible for this policy, whom would you ask for clarification if you are unsure?**

*The responsibility should be shared between Ministry of health and the hospital. The Ministry needs to provide the strategy and guidelines of the policy. They are the main decision makers in the Kingdom. On the other hand, the hospital should take the Ministry guideline and implemented in the hospital based on its need and activities.*

**Q26: If access is controlled as part of the system you are using, who is determining the access rights?**

*The access control of the system controlled technically by the ICT department. ICT department takes instruction from the hospital senior management.*

**Q27: Are you aware of any security risks arising from the use of EPR.**

*From personal experience based on my observation, the main risks arising from use of EPR, I have seen staff forget to log off from their*

*machine after their entries and leaving the EPR opened. This may be opportunity for intruder to access EPR and abuse the system.*

**Q28: Are you/ your organization actively addressing any of these risks? If yes, how?**

*This is not part of my job, although I advice staff to be careful from such behavior. To be honest there are people do not like to tell them such thing. They upset if you tell them your act is wrong. This makes some of us keep quiet to avoid conflict with colleague. This of course mainly due to lack of appropriate information security policy.*

**Q29: Have you experienced any situations were you feel a patient's privacy was at risk? Can you identify the part of the EPR system that failed to protect the patient?**

*Most of my experience is based on my observation experience. They are related to the staff practices as I said such as leaving their PC logged on, sharing the monitor with colleagues and so on.*

## Interview No 4

**Q1: Does your organization store and process patient records electronically?**

*Yes, We have electronic system to support patient care. The system has been bought from America and we have staff from the hospital trained on the system in America. From using EPR, most of our patient medical record carried out electronically. It is quiet useful and saving a lot of time and effort. Although the current EPR is still not perfect but it does a good job. We are still in experience process. It needs time and effort to use the full potential of EPR.*

**Q2: Do you have access to these electronic records?**

*Yes, of course. In fact, all the hospital physicians have access to EPR. In fact I use the electronic record in daily basis.*

**Q3: What are the information elements of the EPR you use?**

*I need to access and use most of the information available on the EPR.* **Such as.** *For example, I need to check the patient personal details to ensure I am treating the right patient and his medical history and allergies. These represent the basis for my action.*

**Q4: Are there any items you think should not be stored in an EPR. Could you please give your reason for this?**

*What I have seen on the EPR, there is no item that I do not like to be included in the EPR. The information are either personal details or medical and both of them are important as an official record.*

**Q5: Are there any items you think should be stored in an EPR that are currently not present. Could you please give your reasons for this?**

*I believe, there is a large space for improving the current EPR. There are several items need to be included. This may include the patient mother name. In Saudi Arabia, use of name is important item in identifying the patient.* **How, there are several items can be used in identifying the patient?** You know, it is quiet used in Kingdom socially as there are so many common names. They prefer using the mother name rather using the others such as date of birth or address. In fact sometimes take time for asking the address or date of birth while the mother name we are finding easy and we receive a quick response from the patient. The other important item is storing all x-ray images and other tests images.

**Q6: Do you have sufficient access rights to a patient's EPR to do carry out your job?**

*Yes, no problem, In fact I have a full access to my patients' EPR available in the system. There is no restriction on my access.*

**Q7: If you do not have sufficient rights, what parts of the record would you need access to and why?**

Not applicable

**Q8: Are there any parts of the record that you have access to that you feel are not necessary for you to carry out your job?**

*There is no item in the current EPR is not necessary to carry out my job, As a medical doctor, any information regarding the patient is important either in the medical actions or in communication with third party relevant to the patient. Put it this way, the medical doctor need full picture of information regarding the patient before taking actions, it helps and facilitate the decision making.*

**Q9: Which items of patient medical record you perceive as being confidential and which not?**

*Patient medical condition and diagnosis need to be kept confidential and should not be accessed by anyone apart from the patient medical physician without the patient consent. It is part of my daily activities. Is there a law regulating uploading patient's record without patient consent*

**Q10: Who do you think is the owner of an EPR**

*In my opinion, the EPR owner and only owner is the patient. It is purely individual personal and medical information. He is the sole owner of his own information.* **What is about the hospital?** *You see, the hospital is a facilitator and provider of the health care. They are not owner. I do believe there are personnel in management argue strongly towards they are the EPR owner. I suggest to ask them this question too.*

**Q11: Who do you think is the owner of information you write into an EPR**

*What I am writing into EPR represents my personal view regarding the patient condition, of course based on the medical tests and information I received during the process. The information itself remains the patient owner. He has the right to use or transfer such information to third party, such as may go to other hospital. Here, it is common the patient transfer such information abroad consultants.*

**Q12 would you allow a patient to read what you are entering in his/her EPR over the course of a treatment?**

*The patient has full right to their medical record and I am strongly to establish a process for the patient to access their medical record. In fact, it is part of the medical care process to inform the patient about his medical condition, medicine and allergies.*

**Q13 Do you allow patients to access to his/ her EPR? (are there any restrictions you are aware of)**

*Yes, I always give the patient full access to his own information at the patient convenient time. I have no any restriction to any information. As I told you earlier, the patient is sole owner of the EPR.*

**Q14: How do you access an EPR?**

*The hospital ICT department established User name and Password for accessing an EPR. I have my own use name and I have set my own password. Using them enables me accessing the EPR at any terminal available in the hospital.*

**Q15: Can an EPR be accessed in any other way?**

*Well, I am not expert in ICT, BUT I believe there is no any other way accessing the EPR other tan using the user name and the password provided by ICT department.*

**Q16: What information can you access in an EPR (are there any restrictions to this access?**

*As explained earlier, I have full access to my patients; EPR. There is no any restriction to my access. I believe this is the case for all hospital physicians. Any how, as I explained to you before, physicians needs full information regarding their patients. Possible, I may have restriction accessing other patients in other hospital or department in which I do not need to access such information.*

**Q17: Are there any restrictions to this access (e.g. the patient must give his consent or dependence on the patient's medical condition)**

*There is no any restriction to my access and as far I know there is no or I have not seen patient consent for accessing his/her own EPR. I think, this may need to be addressed as part of the patient*

*right. May be the hospital needs to establish a process for the patient consent.*

**Q18: Can you pass your access rights to someone else (if yes, are there any restrictions)**

*No, I have no right to pass my own right access to somebody else. It is against the hospital rules and regulations. The access privilege remains personal and should not passed to anybody internally or externally. In simple language I have no right to pass my access right to somebody else and ethically is wrong.*

**Q19: Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)**

*Yes, I can add new information, you know and understand, part of job, is entering the new information to the EPR. I need to update the information based on the new medical tests and diagnosis. I need to stress, I can not modify, change or delete previous, already exists, on the EPR. The system does not allow us.*

**Q20: Can you modify/change/delete entries others have made to an EPR (if yes, are there any restrictions)**

*No, I have no right to modify, change or delete others entries. Again, the system doe not allow me. At the same time, I do not need to do so. Why somebody change somebody else entries. It is wrong and bad practice.*

**Q21: Can you comment on entries in an EPR?**

*The current EPR design needs to be changed to make more easy to use and clearer. I found it difficult to navigate and search for information for patient with long medical history.*

**Q22: Is your access to the EPR logged and audited?**

*No as far I know, I have not seen one and nobody told me. May be the management know about auditing process and procedure within the hospital.*

**Q23: Have you been trained on the information security aspects of your EPR system?**

*I wouldn't called a training, I would say I have introduced to the EPR through my senior. He showed how to sue the EPR through and example and watching carrying one or two entries. In brief, I have not been in any official training course. To be honest, I do not need one, it seems easy.*

**Q24: Have you been given a security policy document for you EPR system?**

*The hospital has certain rules and procedures for security policy. I have been given the document but I believe the document needs improvement and updating. There is no clear reliability and security related issues.*
**Sorry, What do you mean? Can you explain**. *There is lack of statement ensuring the reliability of the system we are using and security. There is a need for guarantee statement from the American supplier of the system and from the hospital ICT department. This is needed to motivate the medical staff and patients to use the EPR system.*

**Q25: Who is responsible for this policy, whom would you ask for clarification if you are unsure?**

*Senior management, the hospital authority, is responsible for the hospital policies and strategy. One of these responsibilities is the policy towards EPR security.* ***What's about if you are not ensure****? I usually ask my senior staff for clarification or one of the medical staff such as the senior nurse.*

**Q26: If access is controlled as part of the system you are using, who is determining the access rights?**

*My access is mainly controlled by senior management based on my job rules. Medical record department particularly is the one who set my access rights.*

**Q27: Are you aware of any security risks arising from the use of EPR.**

*The main risk is the possibility of breaching patient privacy. Traditional patient medical record is difficult to cope, transfer, copy and edit. In other hand, the EPR is opposite. Therefore, I stress the main risk of using EPR is the possibility of breaching patient personal and medical information. From personal experience based my observation, the main risks arising from use of EPR, I have seen staff forget to log off from their machine after their entries and leaving the EPR opened. This may be opportunity for intruder to access EPR and abuse the system.*

**Q28: Are you/ your organization actively addressing any of these risks? If yes, how?**

*Medical record department is addressing any security issues and deal with it accordingly. However, there is no clear policy and or strategy*

*on security policy. I feel the hospital needs a well structured system in addressing risks. At the moment, I feel still not under control. I feel, there is a need bringing, the hospital management, EPR users and ICT department to discuss and establish process for addressing risks issues, I am just suggesting!*

**Q29: Have you experienced any situations were you feel a patient's privacy was at risk? Can you identify the part of the EPR system that failed to protect the patient?**

*As I explained earlier, the main experience I got regarding the patient privacy' is mainly due to misuse of the EPR. Some time, member of medical staff leave their PC logged on with EPR open and leaving their desk. I feel, this expose the patient privacy at risk. The other situation I experienced is the access control needs to be more restricted.* **For example***, I have seen nurse with full access to EPR. I believe each staff should only allowed to access what he needs based on his/her job role and responsibilities.*

## Interview 5,

**Q1: Does your organization store and process patient records electronically?**

*One of our main strategy as hospital is to automate our operation to improve our operations performance and focus more on improving patient healthcare process. This reflects our government vision towards e-health services. The first step towards this strategy we have implemented and used EPR system in our hospital to improve our hospital processes and improve patient health care. Our hospital is one of the first hospital to adopt such strategy.*

**Q2: Do you have access to these electronic records?**

*Yes, I have full access to the EPR based on profession needs.*

**Q3: What are the information elements of the EPR you use?**

*As a consultant and I lead teams of professions I need to use all information available in the EPR. This gives me the opportunity to take appropriate decision towards my patient client.*

**Q4: Are there any items you think should not be stored in an EPR. Could you please give your reason for this?**

*The current information of the EPR is excellent step towards a comprehensive EPR system. Currently, there is no items that is not necessary added to the system. However, any information regarding to patient is important in decision making even non-medical information. The only issue these information need to be classified to some sort of files or files, if you know what I mean.*

**Q5: Are there any items you think should be stored in an EPR that are currently not present. Could you please give your reasons for this?**

As you aware from your experience in the West, there are new technology in health services that can be adopted as part of the EPR. This may include all images, videos and operations that carried out in hospital should be included in the EPR to give the senior medical staff tools for appropriate decision making.

**Q6: Do you have sufficient access rights to a patient's EPR to do carry out your job?**

*As senior medical staff, Yes I have access right to a patients; EPR to carry my duty in the hospital. In fact the EPR developed to help to carry out our duty appropriately.*

**Q7: If you do not have sufficient rights, what parts of the record would you need access to and why?**

Not applicable

**Q8: Are there any parts of the record that you have access to that you feel are not necessary for you to carry out your job?**

*There are items I do not use but not necessary it means they are not necessary to be included in the EPR. As a consultant and a leader of a medical team, I need to access and consider the medical items and any information that helps me to take a profession medical decision. From personal view, any information in the EPR will be helpful in healthcare process or from managing patient care.*

**Q9: Which items of patient medical record you perceive as being confidential and which not?**

*Look, all items in the record are private information and should be considered as private document. Nobody is happy to pass his information to third party without his permission even his or her name. The EPR items should be perceived as confidential document. The record should be accessed only by staff who involve directly in the patient's health care process. The staff access should have access Only on the information that they need to carry out their job and they should not be allowed free or open access to the EPR. We may have open access now, in principle is wrong and needs to be changed. I am aware may be there is a technical problems and I will leave this to ICT department to discuss this issue with you.*

**Q10: Who do you think is the owner of an EPR**

*Well, it is a good question. It is difficult to say who is the owner of the EPR as we are in SA NHS still has no clear policy and legislation to clarify the ownership and access rights and so on. This may be we are still in process of developing our NHS. Of course, we as organization, we create and develop the EPR and we are responsible for its content and development. In the other hand, the information is purely related to private, personal individual. It can be argued is the patient is the owner of the EPR. In brief, we need a definition and regulation to clarify the issue. However, from my personal view the owner of the EPR is the patient and this should be regulated in our NHS services.*

**Q11: Who do you think is the owner of information you write into an EPR**

*The information that I write in the EPR system is purely is based on my knowledge, experience and profession judgment. Legally, I am responsible for the information. On the other hand, the information is purely related to the patient case. In principle, the information I write should be owned by the patient.*

**Q12 would you allow a patient to read what you are entering in his/her EPR over**

**the course of a treatment?**

*In my personal practice, yes I let the patient read his her own record, If you ask do they have the right, I would say yes ff course, the patient is the owner of his/her personal medical record. The hospital role is focused in medical care and the information is purely to help this care.*

**Q13 Do you allow patients to access to his/ her EPR? (are there any restrictions**

**you are aware of)**

*We are on the early stage of establishing clear policy regarding the patient right compared with developed country. However, we are in the right track. We have started several steps towards patient right, such us encouraging staff to brief the patient about his medical case as an example".* (Interviewee 5, Consultant)

**Q14: How do you access an EPR?**

*The process for accessing the EPR is traditional using technical approach control. What I meant is by using the normal process for accessing PCs using username and password. I have my personal username and password and I use them at each time I log on the system.*

**Q15: Can an EPR be accessed in any other way?**

*Technically should not be possible unless by a hacker. One of the disadvantages of using technology is changing and possibility someone somewhere will have the experience and knowledge to access your system. Based on my personal experience, I would say no it cannot be accessed by any other way.*

.

**Q16: What information can you access in an EPR (are there any restrictions to this access?**

*I have full access right to the EPR system and there are no any restrictions to my access right. This is possibly due to my role in the patient's healthcare process.*

**Q17: Are there any restrictions to this access (e.g. the patient must give his consent or dependence on the patient's medical condition)**

*As explained, there are no restrictions to my access to the system and I do nor need to have permission from any one as I am the creator of the information. Of course, I do access unless I am in*

*process of providing professional judgment for the patient. In transferring the records, printing and so on, yes I believe we need to take permission from the patient. Currently, the patient and the organization are not aware of the importance of such process, taking permission from the patient before transferring and printing EPR.*

**Q18: Can you pass your access rights to someone else (if yes, are there any restrictions)**

*Access right is personal and should not be passed to a third party. This is against the ICT department regulation and could have legal implications. In principle, I can pass my username and password to somebody else to use in my absent.*

**Q19: Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)**

*I can create the entries, yes I can write and express my views and my medical decisions. Once I save the information I cannot modify, change or delete the information.*

**Q20: Can you modify/change/delete entries others have made to an EPR (if yes, are there any restrictions)**

*Definitely not, It is not possible from technical point of view, the system will not allow me to do so and from professional point of view, no body should modify or change entries of fellow profession. It is not right and illegal and nobody should do it.*

**Q21: Can you comment on entries in an EPR?**

*After experience and using of the current EPR, the staff feel there is a need to be modified to reflect the hospital and staff needs to facilite the hospital operations.*

**Q22: Is your access to the EPR logged and audited?**

*No doubt, it is critical to our continuous patient health care improvement process to carry out auditing to identify our strengths and areas for improvements. I do believe we need to be robust on out auditing process"*.

**Q23: Have you been trained on the information security aspects of your EPR system?**

I am one of the staff who went to USE to evaluate and train on the system. I have a good introduction to the system and its functionality. You know short training courses is not the same as using the system in daily based to meet the patient needs.

**Q24: Have you been given a security policy document for you EPR system?**

*We do not have EPR specific policy to hand in to the medical and non-medical staff. This is may be due to the system is relatively new. We have a generic ICT policy in which everybody got a copy once they got the log on username and password.*

**Q25: Who is responsible for this policy, whom would you ask for clarification if you are unsure?**

*In principle, the information security policy should be part of the hospital and national vision and strategy, The responsibility relies on the Health Ministry is the main health services authority, NHS is a public in SA sponsored and managed by the government. Beside that national responsibility, the hospital also has responsibility to establish information security to reflects its departmental needs.*

**Q26: If access is controlled as part of the system you are using, who is determining the access rights?**

*The access to EPR controlled by two ICT department and senior management. I would say the ICT mainly do the technical part of the access control and the mangment decide to access. This is usually based on the employee job description and needs*

**Q27: Are you aware of any security risks arising from the use of EPR?**

*The risk can be generated from the staff information seeking behavior. I have seen staff go to other staff and look at his monitor to get certain information regading a patient. Possibly, they need to save time and effort. In principle this should not be happened. Lack of monitor, substation, has led to staff sharing information in which in my view is a bad practices*

**Q28: Are you/ your organization actively addressing any of these risks? If yes, how?**

*Part of my job, I usually advice my team and informed regarding bad information security practices. As you aware, we are as consultants are vet busy and this should not be part of our job. Organisation has not done enough to address risks issues yet.*

*The EPR is critical confidential document and the hospital should take all the measures to ensure its confidentiality.*

**Q29: Have you experienced any situations were you feel a patient's privacy was at risk? Can you identify the part of the EPR system that failed to protect the patient?**

*Yes, the example I gave you in my answer in the previous question. Lack of substations in some wards, especially for the nurses has led to share the PC station and share information on the screen.*

## Interview No 6

**Q1: Does your organization store and process patient records electronically?**

*I am relatively new to the hospital*. How long you have been working in the hospital? *I could see just over two years experience in this hospital however, I used work with other SA hospital before joining this hospital and two answer your question I could say yes this hospital use electronic means for recording and storing patients information. In fact, I surprised at the first time when I saw it in this hospital as the hospital I used work for in SA they are using purely papers and files system into their patient storing and recording process.*

**Q2: Do you have access to these electronic records?**

*It depends in what you mean by access. In principle I confidentially can say that I have right to access EPR but not in full. I believe, the hospital is still has no technical and policy for EPR access control. I believe we need to access more information regarding the patient records*. We will come to this in other question. Let me ask you another question.

**Q3: What are the information elements of the EPR you use?**

*They are several items of the EPR I need to use part of my job role. The most important information is the patient's personal details. I need to check these information with the patient before I start any tasks with the patient. This is part of our job principles and guidelines. I also need to use the consultant and physicians decisions and instructions in what to do as a nurse*. Can you explain what do you mean by that and give me example if you can please? *This include patient medicine dose, and time of giving medicine to the patient, checking the patient blood pressure as another example.*

**Q4: Are there any items you think should not be stored in an EPR. Could you please give your reason for this?**

*From my relative experience and knowledge in the system I can not think about any at this stage as I have no full access to the EPR system,*

**Q5: Are there any items you think should be stored in an EPR that are currently not present. Could you please give your reasons for this?**

*Patient religion needs to be stated in the EPR to help in respecting the patient belief and to help him/her in practicing his religions … The most important is also the needs to take the right actions on case the patient death.*

**Q6: Do you have sufficient access rights to a patient's EPR to do carry out your job?**

*Again, I cannot comment in this but generally I would say NO.*

**Q7: If you do not have sufficient rights, what parts of the record would you need**

**access to and why?**

*Currently our access is limited and we do not have full access of the patient's medical history and details of diagnosing. The current access mainly I could put as instruction in what do with the patient rather accessing information to help understand the patient case thoroughly.*

**Q8: Are there any parts of the record that you have access to that you feel are not necessary for you to carry out your job?**

*No*

**Q9: Which items of patient medical record you perceive as being confidential and which not?**

*If you want my personal view in this, I can tell any that all the patient medical details should be kept confidential and the patient personal details are not confidential but this is not up to me to say. This is the hospital management strategy.*

**Q10: Who do you think is the owner of an EPR**

*Without hesitation is the patient.* This is quick answer, Why not KFH?. *Oh yap you can argue is the hospital owner. In my personal view, the hospital is a tool for processing and creating the information but they are not the owner.*

**Q11: Who do you think is the owner of information you write into an EPR**

*The same answer to the previous question, patient.*

**Q12 would you allow a patient to read what you are entering in his/her EPR over the course of a treatment?**

*I am aware and believe in patient right. The EPR is purely their personal medical information. From my part on the patient right process, I have guidelines to follow regarding the patient right.*

**Q13 Do you allow patients to access to his/ her EPR? (are there any restrictions you are aware of)**

*I am aware and believe in patient right. The EPR is purely their personal medical information. From my part on the patient right process, I have guidelines to follow regarding the patient right.*

**Q14: How do you access an EPR?**

*Well, we have PC stations in our wards and simple we log on to the system normal way*. What do you mean by normal way? *What I meant is using the log on password and user name given by the hospital ICT department.*

**Q15: Can an EPR be accessed in any other way?**

*No as far I know.*

**Q16: What information can you access in an EPR (are there any restrictions to this access?**

*As explained earlier mainly the patient personal detail in which I use them as part of the process for identifying patient and instruction from the physicians and consultants in what I need to do with the assigned patient.*

**Q17: Are there any restrictions to this access (e.g. the patient must give his consent or dependence on the patient's medical condition)**

*As far as I am aware there is no any restriction in the information set for me and I am not aware and have not seen any patient consent in the hospital.*

**Q18: Can you pass your access rights to someone else (if yes, are there any restrictions)**

*From personal and moral, I can stress that I highly rate the EPR confidentiality. The medical part of the record should only accessed by the hospital medical staff. I will never pass any information to another else. If you ask me technical I could say simply pass my user name and my log on password.*

**Q19: Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)**

*Firstly, I cannot delete, change or modify any information of the EPR if I have completed the task and pressed save. The system does not allow me to do it after that. The only permission I have given is to record the patient blood pressure, heart beaten rates and temperature. I also record the patient medication taken date and time.*

**Q20: Can you modify/change/delete entries others have made to an EPR (if yes, are there any restrictions)**

*No, I cannot delete, change or modify any information of the EPR created by other hospital staff. Once the information inserted and saved the system will lock the information.*

**Q21: Can you comment on entries in an EPR?**

*From personal experience, the EPR needs to be developed further. This is from the design and from the content point of views. It needs to be easily used with full patients' details and controlling access rights.*

**Q22: Is your access to the EPR logged and audited?**

*As far I am aware my access is not logged and I never seen auditing process in my ward. You should forgive me, this may be done by higher level of the management but in my personal view I have not seen or observed one.*

**Q23: Have you been trained on the information security aspects of your EPR**

**system?**

*When I joined the hospital two years ago I have no experience in using the hospital system. I have trained in my first week of the job by member of the ward staff, I would say I trained in-house training programme. The staff who trained me was trained in the system in USA. I also like to stress the training programme was short and mainly showed how the system work.*

**Q24: Have you been given a security policy document for EPR system?**

*No I have given one, I have been given an ICT policy. It is a generic guidelines nothing to do with EPR.*

**Q25: Who is responsible for this policy, whom would you ask for clarification if you are unsure?**

*I do not know but I guess the ICT department and If I am unsure for any part of policy or any part of my job I usually as my colleagues and then my senior nurse for clarification and to be honest they usually they do not know when it comes EPR policy.*

**Q26: If access is controlled as part of the system you are using, who is determining the access rights?**

*I am not sure but I have given the user name and password by ICT department after giving them my appointment contract, the hospital management decision on my job role and description.*

**Q27: Are you aware of any security risks arising from the use of EPR.**

*Sure, there are several security risk can be arise from using EPR. This is due to the nature and format of the records. The records can*

*be printed… can transferred to other and can give access right to others.*

**Q28: Are you/ your organization actively addressing any of these risks? If yes, how?**

*For myself as I said my principle as profession in medical care services I will not allow any risk to the EPR. I also I will tolerate any misuse of the EPR and report any risk to my senior nurse. The organization way to address the risk mainly is threatening the staff for any wrong doing.*

**Q29: Have you experienced any situations were you feel a patient's privacy was at risk? Can you identify the part of the EPR system that failed to protect the patient?**

*My only observation, I have noticed the EPR records passed to different people without formal permission from the patient and ward authority. I have also observed a common to share the monitors by member of medical and non-medical staff as well as leaving the computer switch on with patient details on the screen.*

## Interview No 7

**Q1: Does your organization store and process patient records electronically?**

*I would say yes we are well in process of implanting electronic system throughout our operations. EPR system is installed and operated in the hospital. We have an American system which I thing is good enough to work on it at this transition time of implementing the hospital e-health strategy.*

**Q2: Do you have access to these electronic records?**

*Nurse needs to access patent's personal details to ensure she is dealing with the right patient and not mixing up with other patient, patient allergies and current diagnosis as examples. I am currently have limited access to the EPR and there is no clear policy stating my access right.*

**Q3: What are the information elements of the EPR you use?**

Based on my job role on the patient's health care process, there are items I need to access to achieve my daily job. The critical part of our job as nurse is identifying the patient's. We achieve this by reading the patients' personal details. Therefore, I am using the patient's personal details as well as reading the patient's medications needs and what to monitor, patient's temperature and blood pressure as examples.

**Q4: Are there any items you think should not be stored in an EPR. Could you please give your reason for this?**

*My view, if the system is secure I can not see any harm of adding any information regarding the patient in fact I feel is a good idea to add any information regarding the patient. This gives a comprehensive information regarding the patient. These information can help patent care process.*

**Q5: Are there any items you think should be stored in an EPR that are currently not present. Could you please give your reasons for this?**

*One of the items that I think needs to be part of the EPR and used in operations and processes is the patient's picture. This helps in identifying the patient's. This is simply my personal view.*

**Q6: Do you have sufficient access rights to a patient's EPR to do carry out your job?**

*I do not know what do you mean by sufficient access right to a patient EPR. I meant sufficient access to carry out your job as nurse properly? In this case I need more access right to achieve my job professionally.*

**Q7: If you do not have sufficient rights, what parts of the record would you need access to and why?**

*I think we need a full read access to the patient record. This helps patient's healthcare process and help to carry out our job properly. Currently. I think nurse profession needs to be valued more in the hospital and this may be not what we to discuss with you.*

**Q8: Are there any parts of the record that you have access to that you feel are not necessary for you to carry out your job?**

*At this stage none.*

**Q9: Which items of patient medical record you perceive as being confidential and which not?**

*I think EPR information needs to be divided based on the confidentiality of the information. Each part of the EPR has its confidentiality weight and value. These may be started with patient personal details, patient non-medical information, Patient medical history, patient's medications and patient's serious illness.*

**Q10: Who do you think is the owner of an EPR**

*I need to think carefully in this question as both the hospital and the patient's are heavily related to the EPR ownership. However, I could say I more lean towards the patient's ownership than the organization ownership.*

**Q11: Who do you think is the owner of information you write into an EPR**

*I strongly believe is the owner of the information and my organization is the creator and processor of such information.*

**Q12 would you allow a patient to read what you are entering in his/her EPR over the course of a treatment?**

*I always in favour of allowing the patient to read his record and understand it. If you ask whether the patient is the owner of his/her record, my answer will be, Of course, the patient is the owner of his/her personal medical record. The hospital role is focused in medical care and the information is purely to help this care*.

**Q13 Do you allow patients to access to his/ her EPR? (are there any restrictions you are aware of)**

*The patient currently does not have access to EPR. We orally informed him regarding what is in EPR record. We let the patient's his/her health process part of professional procedure but there is no policy or guidelines allowing patient access to the EPR.*

**Q14: How do you access an EPR?**

*I am accessing the system through the traditional access procedure. I have given username and password. These usually set by the hospital ICT department*

**Q15: Can an EPR be accessed in any other way?**

*Technically and as far I am aware of the system cannot be accessed by any other way.*

**Q16: What information can you access in an EPR (are there any restrictions to this access?**

*I access few items of the EPR. I have access to the patient's personal details and reading comments and instruction regarding the patient's written by the physicians and consultant. The main restrictions are I cannot write, update or delete any information written.*

**Q17: Are there any restrictions to this access (e.g. the patient must give his consent or dependence on the patient's medical condition)**

*No, none, the hospital has no guidelines or policy regarding the patient's consent. I am also not aware of any formal restrictions.*

**Q18: Can you pass your access rights to someone else (if yes, are there any restrictions)**

*No I cannot pass my right to other users, internally or externally. This is part of the ICT policy.*

**Q19: Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)**

*I have limited access and limited right to write. I have some access to record patient's monitoring data such as patient temperature and blood pressure. I cannot change them or delete them onece they are saved in the system.*

**Q20: Can you modify/change/delete entries others have made to an EPR (if yes, are there any restrictions)**

NO, I cannot. Firstly, the system does not allow me to change or delete as well as Why should need to change it. This is wrong practice and should not allowed anyhow.

**Q21: Can you comment on entries in an EPR?**

*The current EPR represents a good start for the hospital and health services in general. As I said, the system bough from America and we are in transition period. I strongly believe the system needs to be updated to reflect the hospital and the patient's needs and satisfactions.*

**Q22: Is your access to the EPR logged and audited?**

*I have not seen or observed one. In simple answer no.*

**Q23: Have you been trained on the information security aspects of your EPR system?**

YES, I am one of the group that trained in USA part of the agreement with system provider. I have learnt about the system during the

training programme. I am helping other if they need a help in how to use the system.

**Q24: Have you been given a security policy document for EPR system?**

*The hospital has no EPR specific policy to give to start with. However, the hospital has ICT policy but not EPR specific.*

**Q25: Who is responsible for this policy, whom would you ask for clarification if you are unsure?**

*Do you mean EPR security policy?, Yes. I believe there is a need for clear national policy followed by the hospital policy to protect the EPR. The national policy should be the responsibility of the government and the second should be the hospital management.*

**Q26: If access is controlled as part of the system you are using, who is determining the access rights?**

*I guess the ICT department as they are the only department able to do such access. Of course, this needs to be dome with the hospital management.*

**Q27: Are you aware of any security risks arising from the use of EPR.**

*The main risk source is the EPR users, I meant the hospital staff information security behavior. They do not take care of using the system, they leave their system one while they are absent for considerable time.*

**Q28: Are you/ your organization actively addressing any of these risks? If yes, how?**

*I am addressing such practices by telling the staff especially as trined personnel in the system. I always mention this bad practice in our regular meeting. The organization unfortunately still has not addressed this problem yet.*

**Q29: Have you experienced any situations were you feel a patient's privacy was at risk? Can you identify the part of the EPR system that failed to protect the patient?**

*I have seen the record passed from one department to another by non-medical staff or between organizations without any serious considerations to the EPR security and patient right.*

## Interview No 8

**Q1: Does your organization store and process patient records electronically?**

*Yes, we do. I can confirm use the hospital store and process patient record electronically.*

**Q2: Do you have access to these electronic records?**

*Yes I have access to the EPR*

**Q3: What are the information elements of the EPR you use?**

*Yes, I do use the EPR, The first contact of the patient with the hospital is through us in the medical reception area. Patient personal details are taking and stored in the EPR*

**Q4: Are there any items you think should not be stored in an EPR. Could you please give your reason for this?**

One of my main job role and responsibility is filling patient personal details in the EPR. This includes patient full name (first name, father name, grandfather name and surname), date of birth, address and first kin.

**Q5: Are there any items you think should be stored in an EPR that are currently not present. Could you please give your reasons for this?**

*I think adding the patient photo to the EPR is a good idea. We need this item as some time facilitate identifying the patient.*

**Q6: Do you have sufficient access rights to a patient's EPR to do carry out your job?**

*I think I have enough access to the EPR to carry out my job. I have sufficient access right to the EPR. I need mainly to enter the patients' personal details.*

**Q7: If you do not have sufficient rights, what parts of the record would you need access to and why?**

*The other part of the EPR I do not need them to carry out of my job. I am happy with my current access right.*

**Q8: Are there any parts of the record that you have access to that you feel are not necessary for you to carry out your job?**

*No. none*

**Q9: Which items of patient medical record you perceive as being confidential and which not?**

*In my view, the whole patient document is confidential as it contain confidential information. The hospital considers this document as confidential and important.*

**Q10: Who do you think is the owner of an EPR**

*I am not sure but I believe the ownership is between the hospital and the patient. We as a hospital develop, mange, design and create the document and therefore we need to be owner of the document. On the other hand, the EPR contains personal details and should owned by the patient. Therefore, I would say shared ownership.*

**Q11: Who do you think is the owner of information you write into an EPR**

*As I said is the hospital from managing the document point of view and the patient.*

**Q12 would you allow a patient to read what you are entering in his/her EPR over the course of a treatment?**

*I would let the patient to read what I wrote if he or she wish to do so. I usually read what I write to the patient to ensure my entries are correct.*

**Q13 Do you allow patients to access to his/ her EPR? (are there any restrictions you are aware of)**

*No, it is not part of the process to allow patient to access his or her record while I am doing my job. It takes time and not appropriate I guess.*

**Q14: How do you access an EPR?**

*I access the system by using username and password giving to me by the ICT department.*

**Q15: Can an EPR be accessed in any other way?**

*No, as far I know you must have username and password to access the system.*

**Q16: What information can you access in an EPR (are there any restrictions to this access?**

*I mainly access the patient's personal details. There is no any specific restriction to this access.*

**Q17: Are there any restrictions to this access (e.g. the patient must give his consent or dependence on the patient's medical condition)**

*There is no restrictions to my access and I do not take permission or patient consent to my system access.*

**Q18: Can you pass your access rights to someone else (if yes, are there any restrictions)**

*No it is not allowed and I should not pass my right to other. Each one in our department has her own access and nobody passes its access right to others. Technically I can pass my username and password to others but this is not part of our practice.*

**Q19: Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)**

*I can during the process of writing the entries but not after completing the entry. The system does not allow.*

**Q20: Can you modify/change/delete entries others have made to an EPR (if yes, are there any restrictions)**

*No, it is not possible.*

**Q21: Can you comment on entries in an EPR?**

All my comment, the entries needs to be presented in much better environment and needs to be well designed to make the system easy to use.

**Q22: Is your access to the EPR logged and audited?**

*I do not know.*

**Q23: Have you been trained on the information security aspects of your EPR system?**

*Yes, I had in house training.*

**Q24: Have you been given a security policy document for you EPR system?**

*Nobody gave a a copy of EPR security policy. To be honest I have not seen one.*

**Q25: Who is responsible for this policy?, whom would you ask for clarification? if you are unsure.**

*I think the responsibility of information security I guess is the hospital management. They are the authority of the hospital authority and they also gets information from Ministry of Health.*

**Q26: If access is controlled as part of the system you are using, who is determining the access rights?**

*Our head of department pass our names for access right to the hospital management. The head of department decision is based on our role on the patient health care process.*

**Q27: Are you aware of any security risks arising from the use of EPR.**

*No, I am not aware of any serious risks arising from the use of EPR. The main concern I have observed several patient's relatives or friend they come and ask about the patient information and record. Some of our staff pass some of the information under pressure from the patient's relative and friend.*

**Q28: Are you/your organization actively addressing any of these risks? If yes, how?**

*Yes, we try hard to stop passing information to the patient's relatives and friends especially we do not know their identity.*

**Q29: Have you experienced any situations were you feel a patient's privacy was at risk? Can you identify the part of the EPR system that failed to protect the patient?**

*As I explained passing information verbally to patint's friend and relative verbally with checking their identity carefully.*

## Interview No 10

## MIS Member-ICT Adimn 1

**Q1: Does your organization store and process patient records electronically?**

*Yes, our department installed the system and the system is now in full operation. This is part of our strategy to use EPR system to support our patient's healthcare operations and processes.*

**Q2: Do you have access to these electronic records?**

*Yes I do have access to the system. This is mainly due to my authority in the system. Also I need the access right to help solving any technical problem of any of the employees.*

**Q3: What are the information elements of the EPR you use?**

*I do not use any part of the EPR system. My role is purely technical. I look after the technical issues related to the system and not using the EPR as part of daily job routine. I may only needs number of patients in the system and other non0medfical information that I may need for statistical or maintenance information. I do not use any of the patient personal or medical information.*

**Q4: Are there any items you think should not be stored in an EPR. Could you please give your reason for this?**

*Sorry, I cannot comment in the EPR items. The items ate mainly medical information and this is not part of my job to evaluate or access the patient medical information. You should ask the medical staff who has access to the EPR system.*

**Q5: Are there any items you think should be stored in an EPR that are currently not present. Could you please give your reasons for this?**

*NO, I do not know. I am sorry I can not comment on the items of the EPR system.*

**Q6: Do you have sufficient access rights to a patient's EPR to do carry out your job?**

*Yes I do have the necessary right to carry out my job. Remember sir my job is technical and I provide solution to the EPR users and nothing to do with the EPR as detailed document. So and in brief I have more sufficient access right to the system.*

**Q7: If you do not have sufficient rights, what parts of the record would you need access to and why?**

*Not applicable*

**Q8: Are there any parts of the record that you have access to that you feel are not necessary for you to carry out your job?**

*I would say most of the EPR record I do not them and not necessary to carry out of my job. The items are medical information and non of the main I need I my job. Most of the information is needed by the hospital medical staff. To be honest in our departments non of us need the access to the EPR./*

**Q9: Which items of patient medical record you perceive as being confidential and which not?**

*From my experience as technologist I believe all the EPR is a confidential document. We need to be sure as hospital this document kept confidential. One of our main job as a department is to protect the EPR and keep the document confidentiality.*

**Q10: Who do you think is the owner of an EPR**

*The main owner of the EPR as I see it is the patient. The patient is owner of the EPR for three main reasons in my views. The first is the EPR contains personal details no body has them and owns them. The second reason is the medical part of the information. It has a medical record that related to the patient only. It is specific information and nobody can claim he owns them. Thirdly, the record should be kept by the patient. This can be achieved by giving the record to the patient after each visit on a USB or email to him to used in his next visit to this hospital or any other healthcare organization*

**Q11: Who do you think is the owner of information you write into an EPR**

*I do not write into an EPR at all. As I explained earlier this is not part of my job. My job is technical only.*

**Q12 would you allow a patient to read what you are entering in his/her EPR over the course of a treatment?**

*Again this is not part of my job and I have any formal or informal medical or non-medical interaction with patients.*

**Q13 Do you allow patients to access to his/ her EPR? (are there any restrictions you are aware of)**

*At the moment, the patient has no access right to their records. It is possible introduced in near future and again this is not part of my job. The patient is not part of my daily working process.*

**Q14: How do you access an EPR?**

*As ICT member staff I have the password and user name that give the full right to access our system including the EPR. I need the access to help the staff to solve their technical problem and set their access to the system.*

**Q15: Can an EPR be accessed in any other way?**

*No there is no other way for accessing the system. The user must have the authorization to the system and the appropriate and valid username and password. The only worry is the possibility of hacker and the good news I have not experience one in our current system.*

**Q16: What information can you access in an EPR (are there any restrictions to this access?**

*I have full access to the system and there is no any restriction to my access. Again I have the access to help in maintaining the system and provides help and support to the system uses.*

**Q17: Are there any restrictions to this access (e.g. the patient must give his consent or dependence on the patient's medical condition)**

*As far as I know there is no restriction to my access to the system and there is no any consent from the patient. This is part of my job set by the hospital management.*

**Q18: Can you pass your access rights to someone else (if yes, are there any restrictions)**

*No it is not possible. Each member of the team has his own access right and should not pass the right to somebody else. This is against our policy and against out working tradition.*

**Q19: Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)**

*Again, it is not part of my job to change the entries of the EPR, nothing to do with my job.*

**Q20: Can you modify/change/delete entries others have made to an EPR (if yes, are there any restrictions)**

*No, it is not possible and I never do that anyhow. It is against my personal principle.* I do understand but I am asking technically can you change it? *No I cannot change it.*

**Q21: Can you comment on entries in an EPR?**

*No I cannot comment, I leave it to the medical staff, sorry for this answer.*

**Q22: Is your access to the EPR logged and audited?**

*Up to now we do not have an audit or logging process in the place. I do believe it is a critical and important to have robust logging and*

*audit systems to trace our activities and identifies our strengths and weaknesses.*

**Q23: Have you been trained on the information security aspects of your EPR system?**

*I am one of the ICT team members who attended a training course in USA as part of our contract with the system developer. I would say I had a good training course in USA that has put me in a good place to serve the hospital system users.*

**Q24: Have you been given a security policy document for you EPR system?**

*In the department we do not have EPR policy written specially to serve EPR system. However, we have ICT policy and the given to each member of the hospital staff.*

**Q25: Who is responsible for this policy?, whom would you ask for clarification? if you are unsure.**

*The ICT team should be responsible for establish and developing appropriate EPR policy. This of course needs to be approved by the hospital management. I am also in favour of involving the medical and non-medical staff representative in the policy developing process.*

**Q26: If access is controlled as part of the system you are using, who is determining the access rights?**

*In our department, the head of department is the one who gave use the access right to the system. One we bought the system, we have trained in how to control the access right. Of course, our head is member of the hospital senior management and you can argue the senior management is also involved in the access control process.*

**Q27: Are you aware of any security risks arising from the use of EPR.**

*I personally and from my personal experience, the main risks arise from the system users and the organization culture. The organization culture today is the main risks to the EPR security. The employees as I have observed they pass patient's information to patient relatives or to other hospital member of staff without any sort of consent from the organization, patient of the department. There is also possibility of internal or external hacker, this is a technical risk.*

*The other main threats to the EPR include copying EPR electronically and using the photocopiers available in all hospital departments, possibility removing and changing some content of the EPR and finally passing the information to third party*

**Q28: Are you/your organization actively addressing any of these risks? If yes, how?**

*As ICT department, we do out best to address any technical issue that may be lead to any type of risks to our system. The hospital bought latest technology for the system safety and security. One of the main challenges of EPR access is the hospital users skills and competence. The vast majority of our daily jobs is helping and supporting staff accessing and use of EPR effectively".* (Interviewee 10, ICT administrator)

**Q29: Have you experienced any situations were you feel a patient's privacy was at risk? Can you identify the part of the EPR system that failed to protect the patient?**

*As I have mentioned earlier. The main risks are coming from the organization culture, employee's behavior. Patients' information passed and handled openly in the hospital.*

## Interview No 11

## MIS Member-ICT Adimn 2

**Q1: Does your organization store and process patient records electronically?**

*Yes, the hospital introduced electronic system to improve the hospital performance and saving time and effort. We are currently store and process patient records electronically. The record start from the time patient enters the hospital till he/she leaves the hospital*

**Q2: Do you have access to these electronic records?**

*The medical record users need a user name and passwords to enter the system. This is usually set by the medical record department at the hospital custodians Personally, I have the right to access patient records; in fact there is no any restriction on my team on the access rights.*

**Q3: What are the information elements of the EPR you use?**

*No, I do need any elements of the EPR to carry out of my job. My job is not related to the use of EPR. MY job role in the hospital is technical and nothing to do with detailed information of the EPR.*

**Q4: Are there any items you think should not be stored in an EPR.**

**Could you please give your reason for this?**

*Ideally, the hospital medical staff should answer this question. The EPR information are medical information and needs to be entered by the medical staff. The items need to reflect the medical staff. Therefre, I suggest to ask the medical staff they will be in better situation to answer this question.*

**Q5: Are there any items you think should be stored in an EPR that are currently not present. Could you please give your reasons for this?**

*I cannot comment into the items needs to be stored. Again I am not in a position to answer this question.*

**Q6: Do you have sufficient access rights to a patient's EPR to do carry out your job?**

*I have sufficient access right to the system. You know without a full access right I may have a problem to carry out of my job. The access allow me to help solving the system users problem as well as facilitate their access right, establishing the access right to the system.*

**Q7: If you do not have sufficient rights, what parts of the record would you need access to and why?**

*Not applicable*

**Q8: Are there any parts of the record that you have access to that you feel are not necessary for you to carry out your job?**

*Again my job is not medical. I do not have any role into the patient healthcare process. I only provide the technical support to the system and the users. I do not need any part of the EPR in my job.*

**Q9: Which items of patient medical record you perceive as being confidential and which not?**

*In my view, patient's electronic record is confidential record. I meant the whole record is confidential. I can not consider one part is confidential and other is not. You understand any information has its level of security. EPR parts are also has its own security level. Some of the parts needs to high index of security than other parts.*

**Q10: Who do you think is the owner of an EPR?**

*I think the owner of the EPR is the medical information department. They are the main developer and implementer of the medical information system. Therefore, they are the sole owner of the EPR.*

**Q11: Who do you think is the owner of information you write into an EPR**

*It is not part of my job to access and write into the patient EPR.*

**Q12 would you allow a patient to read what you are entering in his/her EPR over the course of a treatment?**

*Not applicable question*

**Q13 Do you allow patients to access to his/ her EPR? (are there any restrictions you are aware of)**

*Not applicable question*

**Q14: How do you access an EPR?**

*I do not access EPR specifically as I do need to access the record. My job does not need accessing the EPR record. I do access the entire system through using username and password as usual.*

**Q15: Can an EPR be accessed in any other way?**

*The system designed and protected from any illegal accessing apart from the authorized access. The system I personally is well secured. However, as you know in technology everything is possible. Technology of today is old tomorrow due to the changes in technology in very short time. The e-health system is in developing process and each year we can have a new and better system.*

**Q16: What information can you access in an EPR (are there any restrictions to this access?**

*I do not access any EPR information as part of my job but I do not have any restriction to accessing the system. If you ask me which part of EPR is important, personally with no doubt in my mind, the most critical information on EPR is the patient personal details, especially the patient mob number as we had a problem regarding patient mob no* in occasion as I observed the case in the hospital.

**Q17: Are there any restrictions to this access (e.g. the patient must give his consent or dependence on the patient's medical condition)**

*There is no any restrictions to my access to the EPR and as far I am aware there is no any consent in place right now.*

**Q18: Can you pass your access rights to someone else (if yes, are there any restrictions)**

*Access right is assigned to me and should not be passed to any other person even my work colleagues. Thus is not part of our practice and fact this is against our policy.* Is there a statement regarding this issue in your policy? *May be not specifically but this is part of our work practice and norms.*

**Q19: Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)**

*It is not part of job. I only provide technical support to the hospital EPR users.*

**Q20: Can you modify/change/delete entries others have made to an EPR (if yes, are there any restrictions)**

*I have the ability to change and modify the EPR but it is not part of my job role and responsibility. This is purely based on my ICT role and rights to access the IS. There is no restriction on my access right. But there is way I will do that. This is against my principle and work ethic.*

**Q21: Can you comment on entries in an EPR?**

*I have not used the EPR as part of my job therefore I cannot comments on the EPR entries. I will leave it to the medical staff to comment on the EPR entries and design.*

**Q22: Is your access to the EPR logged and audited?**

*We do not have in place processes and procedures for auditing and logged our access to the EPR. It is needed and we should establish a robust and well designed processes and procedures.*

**Q23: Have you been trained on the information security aspects of your EPR system?**

*I have been on a medical training programme in USA. One of the training elements is the medical electronic protection*

**Q24: Have you been given a security policy document for you EPR system?**

*No I do not have a copy of the EPR policy. However, as ICT professional we have the awareness and understanding of EPR policy, However, we have an ICT policy but we do not have ER policy*

**Q25: Who is responsible for this policy?, whom would you ask for clarification? if you are unsure.**

*Our team is responsible for developing the ICT policy and we should also be responsible for establishing the EPR policy. We are the most expert in the information and security. The senior management they need to be involved from the strategic planning point of view.*

**Q26: If access is controlled as part of the system you are using, who is determining the access rights?**

*Our department is the one to determine the access right from the technical point of view. Of course, the hospital management is also part of the process as they role and job description for all the hospital employees. The technical access control is based on the hospital employee's job role in the patient healthcare process.*

**Q27: Are you aware of any security risks arising from the use of EPR.**

*I am quite aware of the risk associated with un-authorized access to the EPR. The risk can be from intern Several times, during my duty to update IS system, I have found PC on with EPR. The user forgot to logout of the system. This is bad experience al or external intruders*

**Q28: Are you/your organization actively addressing any of these risks? If yes, how?**

*My role in addressing the issue is mainly by educating people by advising them regarding any risk issues. The organisation has not addressed such issues as is still not considered as critical from the management point of view.*

**Q29: Have you experienced any situations were you feel a patient's privacy was at risk? Can you identify the part of the EPR system that failed to protect the patient?**

*The main risk is the risk associated for the system users. I do not think the risks come from the system main users. It is still not part of their work practices norm taking the EPR information security seriously. I have observed they felt is norm to pass patient information to any of his relatives or friends without patient consent*

# Interview No 12

# Pharmacist 1

**Q1: Does your organization store and process patient records electronically?**

*Yes, out hospital has implemented EPR system in the hospital as part of its strategy to improve the hospital performance. The hospital pharmacy department has access to the medicine part of the system.*

**Q2: Do you have access to these electronic records?**

*I have only access to the patient's medicine part. I check the medicine and record what have been released from medicine to the patient. I personally do not have a full access to the record only in what I need to do as part of my job.*

**Q3: What are the information elements of the EPR you use?**

*I only use patient's medication section of the system. I need to read and check the medication written by medical staff. Of course I need to check the dose, type of medicine and so one.*

**Q4: Are there any items you think should not be stored in an EPR. Could you please give your reason for this?**

*From my limited access and experience in the system, I cannot identify items that no need to add them to the system. This is purely based on my personal opinion and understanding.*

**Q5: Are there any items you think should be stored in an EPR that are currently not present. Could you please give your reasons for this?**

*I think there is a need to add the patient picture as part of the pharmacist patient's identification process. You understand given the medicine MUSt be give to the right patient. Patient picture helps in identifying the patient clearly.*

**Q6: Do you have sufficient access rights to a patient's EPR to do carry out your job?**

*From my job role perspective, I would say Yes. I need only the medicine type, dose and so one. My job process and making decide mainly on such information and the current system provide such information without any problem.*

**Q7: If you do not have sufficient rights, what parts of the record would you need access to and why?**

*I think, I have sufficient access right to carry out my job properly. I need only the patient's medication section and his/her personal details. I do not need the other section. This is mainly to provide the patient with the right medication based on the medical staff prescription.*

**Q8: Are there any parts of the record that you have access to that you feel are not necessary for you to carry out your job?**

*None as I do not have access to the patient's medical records details. Possible of his personal details I do not need to use them but sometime is good idea to leave them to check the patient's identity in case of a confusion.*

**Q9: Which items of patient medical record you perceive as being confidential and which not?**

The patient medical record is confidential record and this hospital and the staff need to think in this way. I think *Patient medical history. Patient condition and patient medication* are the most confidential items of the record.

**Q10: Who do you think is the owner of an EPR**

*We are the hospital, NHS, are the owner of the EPR. The EPR created by our professional staff, stored and maintained by our organization. The only body who has right to pass store and transfer the record is the organization itself.*

**Q11: Who do you think is the owner of information you write into an EPR**

*The patient is the owner of his or medication prescription. The medication report and details of the patient's medication prescription are purely patient's ownership.*

**Q12 would you allow a patient to read what you are entering in his/her EPR over the course of a treatment?**

*Yes, I read and show the patient is he closes to the monitor his medication. I also need to explain in details the medication. I have to make sure the patient understand his or her medication before he leaves the pharmacy. I also write the details to the nurse in case the prescription is for patients in the hospital ward.*

**Q13 Do you allow patients to access to his/ her EPR? (are there any restrictions you are aware of)**

*The patient has enough information to their medical record through their medical doctor. They provide the patient regarding their medical conditions and the medicines need to be take. Personally,*

*is not part of my job to allow the patient access to hi or her EPR record*

**Q14: How do you access an EPR?**

*I access the system through our pharmacy department. I have the user name and the password. These are needed to access the system. I have got the user name and the password after a filling form from the hospital ICT department.*

**Q15: Can an EPR be accessed in any other way?**

*In our department and the rule we have, there is no any other way for accessing the system. I believe the system is highly secured and there is now way to access apart from using the appropriate username and password set by the ICT department.*

**Q16: What information can you access in an EPR (are there any restrictions to this access?**

*I have access to the patient's personal details and the medication section; purely I have access to the patient's prescription. As far I am aware there are no any resections to my access.*

**Q17: Are there any restrictions to this access (e.g. the patient must give his consent or dependence on the patient's medical condition)**

*No there is no any restriction to this acces and we do not have any process for taking permission from the patient to access his or her medical prescription. We are provider of medication and I believe there is no need in this case to take patient's permission.*

**Q18: Can you pass your access rights to someone else (if yes, are there any restrictions)**

*I cannot pass my access right to somebody. I do not pass and give my username and password to somebody. It is not right and against our practice in this department.*

**Q19: Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)**

*No, I can not change or modify any of my entries once they are in the system. It will become part of the patient's medication section.*

**Q20: Can you modify/change/delete entries others have made to an EPR (if yes, are there any restrictions)**

*Not at all, I cannot do anything with the medical staff entries such as the patient's medication. The system does not allow it and anyhow nobody should give himself the right to change somebody else entries.*

**Q21: Can you comment on entries in an EPR?**

The EPR we are using is good and meet our need. From developing further, yes its is possible to make more attractive and easy to use. There are few items can be added to the system to make more useful to the pharmacy department.

**Q22: Is your access to the EPR logged and audited?**

*I think all our record is logged for future checking as our department very sensitive. All our given medicine can be traced by*

*our professional department and logged electronically for future checking. I have not seen an audit to the current system. This may be due to lack of experience and needs at this particular system and time.*

**Q23: Have you been trained on the information security aspects of your EPR system?**

*I had a brief introductory to the system. It wasn't formal training. One of my colleagues showed me how to use the system in few minutes. Of course, as a pharmacist I used to have some previous experience in using electronic system.*

**Q24: Have you been given a security policy document for you EPR system?**

*No, I have not seen EPR policy in our department and nobody given me a policy regarding the EPR system that I am currently using. I think is excellent idea for exploring the policy issue and you need to raise the issue with the hospital management.*

**Q25: Who is responsible for this policy?, whom would you ask for clarification? if you are unsure.**

*The information security policy should be the hospital responsibility. The hospital management should consult and liaise with the hospital department to establish effective information security policy. I also believe each hospital department needs to establish their own information security policy to reflect their need as each department need specific items.*

**Q26: If access is controlled as part of the system you are using, who is determining the access rights?**

*The department management control our access right. They right to the hospital senior management to set our access right. I would say our department is the one who decide our access right. ICT department provide us with the technical access right.*

**Q27: Are you aware of any security risks arising from the use of EPR.**

*The main risk of using EPR is the entries errors. If a typing error occurred in the process will be very difficult to be checked. This may include the dose of the medicine or type of medicine. Therefore, our job needs to be checked twice and we need to be highly skilled in using the EPR system.*

**Q28: Are you/your organization actively addressing any of these risks? If yes, how?**

*As I explained in my previous question, the major risk in our profession is the medical errors. It is possible due to electronic entries, especially in the kingdom, there are large number of patient's with similar surname and first name.*

**Q29: Have you experienced any situations were you feel a patient's privacy was at risk? Can you identify the part of the EPR system that failed to protect the patient?**

*Most of the patient's presicbtion currently is given with a print out. The print out can be read by different people in the department. Also the patient medication can stay on the monitor and can be seen by different people in the department.*

# Interview No 13

# Pharmacist 2

**Q1: Does your organization store and process patient records electronically?**

*Our pharmacy department implemented EPR system in our process of providing medicine to the hospital in and out patients. The system is currently in operation and part of our daily activities.*

**Q2: Do you have access to these electronic records?**

*Yes I do have access to the system otherwise I cannot do my job. Access to the system is my first activity of the day. Once I start the job I access the system as we do not use paper system any more.*

**Q3: What are the information elements of the EPR you use?**

*My job mainly is providing the appropriate and right medicine to patient based on the medical doctor prescription. Therefore, I only use the patient's identification element of the EPR system to help identifying the patient and the prescribed medicine.*

**Q4: Are there any items you think should not be stored in an EPR. Could you please give your reason for this?**

*From what I need and what I have experienced from the system, there is no item currently stored in the EPR system which is not important from the information I used.*

**Q5: Are there any items you think should be stored in an EPR that are currently not present. Could you please give your reasons for this?**

*Nothing I can remember now, but to help us more in identifying the patient it will be good idea to add the patient picture on the EPR*

*system. The system will be nice and good to have the picture of the patient as part of the patient's identification process.*

**Q6: Do you have sufficient access rights to a patient's EPR to do carry out your job?**

*Yes I do have efficient to carry out my basic job BUT I may need more information. Therefore, If I need to be precise I may need more information to carry out my moiré effectively. There are certain information If it available to me it will facilitate my job process.*

**Q7: If you do not have sufficient rights, what parts of the record would you need access to and why?**

*As I explained in my past answer, I strongly believe there is a need more access to the EPR information. The main information which I need to access is the patients' allergies and patient medical history. Currently, I have to check with the patient's or I have to write a notice on the medicine label.*

**Q8: Are there any parts of the record that you have access to that you feel are not necessary for you to carry out your job?**

*As far I am aware, there is no item I do not need that currently in the system. Most of the items we need to identify the patient identity. Of course, there are I can call critical information such as the full name and date of birth the other items we need them in case we to ensure the identity of the patient if I am in doubt. The information regarding the patient medicine all of it is critical in the system.*

**Q9: Which items of patient medical record you perceive as being confidential and which not?**

*I think and you agree with me the entire patient medical record is confidential record and there is no part of the record can be considered not confidential. However, the question remain for the hospital is which should be part of the hospital policy is "Which part of the EPR record can be released and to whom/ The answer to this question should decide the level of the confidentiality of each item of the record.*

**Q10: Who do you think is the owner of an EPR**

*The owner of the EPR as I understand it is the patient. The medical record is related to one person. It has his or her personal and medical records. Therefore, I cannot see anybody can claim the ownership of the record.* What is about the hospital ownership? *In my personal view, the hospital is not the owner of the record. The hospital for me is the origination that create the record and not the owner. There is a difference between the owner of the record and the system that created the record. Any howm this is my personal view.*

**Q11: Who do you think is the owner of information you write into an EPR**

*I still believe the patient is the owner of the record. My job is adding information to the record. MY job is paid by the NHS and there is no way I can claim I am own it. NHS is also been paid by his majesty government as part of the part government commitments to the Kingdom citizens.*

**Q12 would you allow a patient to read what you are entering in his/her EPR over the course of a treatment?**

*It is part of my job to explain to the patient in details his or her medicine. It is patient right to know and understand the medicine he or she is taking. In fact, I do release the medicine to the patients unless they understand their medicine very well usually, the patient does not want to read in what is the system. However, id the patient wish to do so I have no objection at all. The Saudi usually do ask to read their record.*

**Q13 Do you allow patients to access to his/ her EPR? (are there any restrictions you are aware of)**

*To give the patient access to their medicine record, no I don't have the power authority or the tool to give the patient right to access to their EPR. As you know, this is not part of our job. They need to get access permission from the hospital management and ICT department?*

**Q14: How do you access an EPR?**

*Well as all the staff of the hospital simply using our normal username and password that given to us by the ICT department through our department approval.*

**Q15: Can an EPR be accessed in any other way?**

*No, it cannot be accessed the user MUST have the appropriate right authorization to access the system. What I meant they must have the appropriate username and password.*

**Q16: What information can you access in an EPR (are there any restrictions to this access?**

*The main information I need to access as part of my job is the patient personal details, this include the patient name, date of birth, sex and so*

*on. I need this type of information to help me make sure the medicine that I am going to provide is to the right patient. I also I have access to the patient medicine stated by the hospital medical staff, patient medical prescription.*

**Q17: Are there any restrictions to this access (e.g. the patient must give his consent or dependence on the patient's medical condition)**

*No as far as I am aware, there is no any restriction to my access. If you talk about the patient consent I would say then. I do not need the patient consent to access his or her record. In simple language we do not have a process or form for patient consent in our department. I do not know about other departments or the hospital.*

**Q18: Can you pass your access rights to someone else (if yes, are there any restrictions)**

*No it is not possible. It is not right to pass my personal access right to somebody else as this may lead to criminal offence. I only take responsibility on my behavior and work on the system*

**Q19: Can you modify/change/delete entries you make to an EPR (if yes, are there any restrictions)**

*Yes in the during the process of the entries but once I save the record I cannot do anything to the entries. The system doe not allow it.*

**Q20: Can you modify/change/delete entries others have made to an EPR (if yes, are there any restrictions)**

*No I can not change of others. Anyhow, Why do I need to change the entries? Anyhow, the system doe not allow me to change the entries of others.*

**Q21: Can you comment on entries in an EPR?**

I have personal interest in software and packages generally. Therefore, I would say the current system needs to be more attractive, more eye catching and more easy to use. Therefore, from the system design point of view there is a need to develop the system more.

**Q22: Is your access to the EPR logged and audited?**

*I personally I have not seen or experienced one BUT I think there is nothing in the process. We are working in very sensitive department and there is a need to logged and audit our work. The logged process can be traced by relating any medicines released and the username. The hospital may be still in early stage to audit the system. I do not know to be honest.*

**Q23: Have you been trained on the information security aspects of your EPR system?**

*I didn't have proper or planned training programme. May be they felt I do not need one. This may be due to what I need from the system it can be shown to me quickly and briefly. Therefore to answer your question, I have a brief introductory to the system and showed me in how to access and use the system by the head of department. This has been done within less than an hour.*

**Q24: Have you been given a security policy document for you EPR system?**

*In our department we do not have an official EPR information security policy. As explained my training was brief and nobody give an official EPE information security policy.*

**Q25: Who is responsible for this policy?, whom would you ask for clarification? if you are unsure.**

*To be honest I do not know exactly. I guess the hospital senior management is responsible to establishing the hospital information security and monitor and supervise department specific policies and procedures for EPR information security.*

**Q26: If access is controlled as part of the system you are using, who is determining the access rights?**

*The access control is part of the hospital management system. The access controlled by the senior management and senior management passes some of its authorizations to the ICT and the hospital department teams.*

**Q27: Are you aware of any security risks arising from the use of EPR.**

*The main risk of using EPR is recording process can be given the patient the wrong medicine. This may happen due to change in the monitor screen while the pharmacist in the process of given the medicine or by reading the wrong record. The other risk is the possibility what is in the system monitor can be seen by unauthorized person within the department.*

**Q28: Are you/your organization actively addressing any of these risks? If yes, how?**

*Of course every single person in our department is trying his or her best to eliminate any medical errors. We have no double checking on the medicine prescription before releasing the medicine to the patient. The other risk is part of the departmental culture related to the individual behavior. We try to advice people not to read in any other people monitor unless they authorized.*

**Q29: Have you experienced any situations were you feel a patient's privacy was at risk? Can you identify the part of the EPR system that failed to protect the patient?**

*The main risk is the screen monitor usually left long time during the process of providing the medicines to the patient. During this time, several people in the department can read what in the monitor.*